4. Закон України ″Про Національну поліцію″ / Відомості Верховної Ради України, 2015, №40-41. – С. 379 // Електронний ресурс. Шлях доступу: http://zakon3.rada.gov.ua/laws/show/580-19.
5. Кримінальний аналіз у діяльності НПУ / Концепції впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою ″Intelligence Led Policing″ // Електронний ресурс. Шлях доступу: www.slideshare.net/NationalPpolice/ss-75925350.

Світличний В.А. - доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент;
Головня А.І. - курсант навчальної групи Ф4-102 Харківського національного університету внутрішніх справ

КРІПТОВАЛЮТА. ЕЛЕКТРОННІ ГАМАНЦІ, ПЛЮСИ ТА МІНУСИ

Як відомо, нині широку популярність набуває віртуальна валюта. Користувачі віртуальних гаманців все частіше та частіше роблять вклади у кріптовалюту. Та наскільки це безпечно? І чи досить розвинуті сучасні технології, щоб так широко використовувати цю валюту?

Кріптовалюта — вид цифрової валюти, емісія та облік якої засновані на асиметричному шифруванні і застосуванні різних криптографічних методів захисту, таких як Proof-of-work та/або Proof-of-stake. Функціонування системи відбувається децентралізовано в розподіленій комп'ютерній мережі. Кількість кіберзлочинів росте з неймовірною швидкістю. Практично кожен місяць ми чуємо з новин про яку-небудь велику атаку, а уявіть, скільки дрібніших відбувається щодня. Олії в цю ситуацію однозначно додає активний розвиток інноваційних фінтех-індустрій. Адже утримувачі кріптовалюти куди "зручніші" жертви ніж уряди або великі корпорації. За повідомленнями Coinbase (найбільша кріптовалютная біржа США), кожен місяць кількість атак на криптовалюти збільшується на 100%. Також багато хакерських атак так і залишаються в таємниці, так як біржі і клієнти не хочуть ставити під сумнів свою репутацію з боку користувачів.

Незважаючи на те, що 14% всіх коштів залучених через ICO проектів на платформі Ethereum (а це $ 1,6 млрд) були вкрадені, тобто приблизно кожен десятий проект зазнав успішну атаку. Наприклад, проект Zerocoin. Один зайвий символ у вихідному коді проекту дозволив хакерам викрасти більше $ 500 тис. «Умільці» просто генерували додаткову кріптовалюту в рамках транзакції до тих пір, поки не були помічені. Або ситуація з сервісом Parity Ethereum, коли хакери скористалися уразливістю системи і вкрали з гаманців користувачів $32 млн. Однак, такі помилки приносять набагато менших збитків ніж фішингові атаки. На жаль, від них не врятує ні антивірус, ні найефективніші системи захисту. Так кіберзлочинцям вдалося викрасти $8 млн під час проведення ICO блокчейн-стартапу CoinDash, зламавши сайт і замінивши адресу для відправки коштів користувачами. Також через

фішингову атаку хакери зламали біржу Bithumb. У той день "пощастило" не тільки південнокорейській біржі, а й гаманцю Classic Ether Wallet. Хакери заволоділи доменом гаманця і зникли з $300 тис.

Спільно з фішинговими атаками хакери люблять використовувати шкідливе ПО, яке дозволяє досить швидко красти величезна кількість коштів. У минулому році на сайті Reddit з'явився пост про криптовалюту, де розташовувалася посилання на сайт CryptoChartiq. При кліці на посилання на пристрій користувача завантажувалося програмне забезпечення, яке просто дочиста списувала кошти з online-гаманців. Ще однією гучною історією стало розміщення шкідливого посилання в пошуковому топі Google, яка обіцяла відвідувачам навчити їх поводитися з кріптовалютою і даркнетом. Далі майданчик перенаправляла відвідувачів на фішингові сайти, крадучи при цьому кріптокошти. Ця хакерська атака була організована власниками ресурсу Darknetmarkets.org. Також останнім часом популярність набирають скріпти для майнінга, боротьбою з якими вже зайнялися розробники Google Chrome. Сподіваємося, що і інші браузери теж підтягнуться. Поки для боротьби з цим видом злочинної діяльності можна боротися установкою спеціальних розширень на зразок AntiMiner, No Coin і minerBlock.

Власник кріптовалют часто зберігає її в електронному гаманці. У вас як у власника повинні бути два ключа - публічний (його ви вказуєте для перерахування вам монет) і приватний (його ви використовуєте для підтвердження транзакцій). На даний момент існують два види гаманців - "гарячі" і "холодні". В "гарячих" гаманцях обидва ключі зберігаються в інтернеті у вашого провайдера, а в "холодних" гаманцях приватний ключ зберігається у вас на пристрої. При цьому не можна сказати, що "холодні" гаманці захистять вас повністю. Використовуйте двухфакторную аутентифікацію для додаткової безпеки, хоча і це не 100%. Тут скоріше грає роль системний підхід і загальна обережність. Зберігайте невеликі суми для витрат на "гарячих" гаманцях, заощадження тримайте на "холодних", не тримайте гроші на біржах, встановіть двухфакторну аутентифікацію, не клацайте по сумнівними посиланнями та використовуйте захищену операційну систему iOS.

Майнери, що використовують обчислювальні потужності користувачів - процесори і відеокарти, потихеньку відходять на задній план, так як це стає нерентабельно. Однак, особливо працьовиті майнери досі можуть на цьому заробляти дуже непогані гроші. Найбільш відомими є ботнети DevilRobber і CoinMiner. При цьому останнім часом набирають популярність скріпти для майнінга, які розміщуються в вихідному коді сайтів.

Як показує практика, основні жертви хакерів - це прості люди, власники кріптовалют. Тобто організовуючи масштабну атаку, хакери сподіваються, що у більшої частини користувачів рівень захисту буде залишати бажати кращого. І досить часто вони виявляються праві. Тому необхідно частіше доводити до користувачів інформацію про те, як захистити себе від хакерських атак.