Переваги, які дає використання руткітів - виконання коду в привілейованому режимі, можливість ховатися від засобів захисту та непомітно перебувати в мережі тривалий час - надто важливі для злочинців, щоб відмовитися від такого інструменту [4].

Список використаних джерел:

1. Що за звір rootkit? [Електронний ресурс]. – Режим доступу : https://ua.softlist.com.ua/articles/chto-za-zver-rootkit/

2. Антивірус Битдефендр [Електронний ресурс]. – Режим доступу: https://bitdefender.ru/

3. Руткіти: еволюція та способи виявлення [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/rootkits-evolution-and-detection-methods/#id2

4. Руткіт: експерт з маскування шкідливого ПЗ [Електронний ресурс]. – Режим доступ: https://zillya.ua/rutkit-ekspert-z-maskuvannya-shkidlivogo-pz

УДК 004.056:55(043.2)

МАЛЯРЕНКО ДМИТРО СЕРГІЙОВИЧ

курсант 1 курсу факультету №4 Харківського національного університету внутрішніх справ

ГНУСОВ ЮРІЙ ВАЛЕРІЙОВИЧ

кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

orcid.org/0000-0002-9017-9635

ШАХРАЙСЬКІ СХЕМИ, ЯКІ НАЙБІЛЬШ АКТИВНІ В НАШЕ СЬОГОДЕННЯ

Незважаючи на кризу, стрімко розвивається кредитно-фінансова сфера. Однак вона не завжди приносить користь для громадян, а й часто потурає аферистам, адже інновації в злочинному світі впроваджуються швидко.

Чорні брокери. Варто тільки засвітити номер мобільного телефону в інтернеті, наприклад на дошці оголошень, з великою ймовірністю він може потрапити в базу шахраїв, які почнуть регулярно дзвонити, з пропозицією поторгувати, на деякій біржі; або застосовують бота, який буде робити прогнози та показувати куди ставити. Головним завданням «брокера», буде заставити скачати деяке програмне забезпечення, в який потрібно буде вкладати гроші й торгувати, де й відбудуться осідання. До речі, можуть запропонувати зайти в фішинговий сайт, де результат такий самий – втрата грошей. Позбутися цих дзвінків можна лише змінною SIM-картки.

Бінарні опціони. Користуючись соціальними мережами, ми бачимо успішних людей, деякі з них є несправжніми «трейдерами», які готові поділитися торговими сигналами до закритих або відкритих груп, по реферальному посиланню. Зареєструючись і після внесення депозиту, люди починають торгувати по його вказівкам на бінарних опціонах. «Трейдери» заробляють відсотки або за рахунок внесеного депозиту, але, зазвичай, за рахунок поразки жертви. Реклама опціонів може бути де завгодно. Шахраї в онлайн-оголошеннях придумують нові, різні види обману, для привласнення чужих коштів. На дошці оголошень, де розміщуються оголошення про товари, вакансії і резюме, обманюють, як покупців, так і продавців. Шахрай правдоподібно оформлює оголошення з уціненим товаром. Коли на цей товар знаходиться покупець, виникає угода, торгівля. Багато які інтернет - сервіси блокують на своїх сайтах чужі посилання, тому шахрай може попросити перенести спілкування в інші соціальні мережі, мовляв, що там більш зручніше. Вводячи в оману, повідсилає відредаговані, взяті з інших мереж фото чужого товару. Коли покупець повірить, шахрай відсилає посилання на фішинговий сайт, який зовні виконаний по одній стилістиці як справжнє онлайн-оголошення, але відрізняється лише посилання. Обдурений покупець вводить данні своєї банківської карти, номера телефону й відправляє ці данні шахраю, якому буде не складно зняти гроші з карти. Щоб не бути обманутим треба бути

уважним, обов’язково читати на сайті інформацію спеціальних розділів, які допомагають впізнати шахраїв.

SCAM сайти. Це сайти де, начебто, розігруються грошові кошти: за компенсацію, проходження незначного опитування, тощо. Щоб нібито отримати ці кошти треба оплатити внески, яких буде незчисленна кількість, де і втратить свої гроші користувач. Скільки б не було проведено транзитних операцій, дані кошти вивести неможливо. Щоб не пійматись на даний проект, треба бути скептично налаштованим. На справжніх проектах з виплати коштів, не треба вносити свої гроші, тому що на всі грошові операції використовуються посередні кошти з виплат.

HYIP проекти (фінансові піраміди). Усі хочуть бути успішними та багатими, найбагатші люди планети рекомендують пасивний заробіток, тобто інвестиція. Існує думка, що кожна людина вчиться на своїх помилках, таким чином, отримуючи безцінний досвід. Але якщо в реальному житті необхідний опит, можна отримати пару раз наступивши на одні і ті, самі граблі, то у інвесторів одна помилка може призвести до втрати всього капіталу. Фінансові піраміди відрізняються від реальних проектів тим, що у них нема реальної діяльності проекта. За статистикою, більшість хайпів закривається протягом 6 місяців з моменту свого старту. Не можна при реєстрації використовувати той же e-mail, який ви використовуєте і для платіжних систем. Це може загрожувати тим, що якщо вашу пошту зламають – то паролі від платіжних систем і електронних гаманців зможуть без зусиль відновити і вивести гроші. І саме обов'язкова умова безпеки – для кожного нового проекту використовуйте різні паролі. Ні в якому разі не застосовуйте один і той же пароль, це може спричинити проблеми. Злом будь-якого вашого облікового запису може дозволити шахраям отримати легкий доступ до акаунтів в інших проектах, а згодом і крадіжку коштів.

Вішинг. Зазвичай телефонні шахраї знаходять номера постраждалих на якомусь форумі або дошці оголошень. Схема надзвичайно проста: шахраї телефонують із незнайомого номера і під різними приводами намагаються:

вивідати дані платіжної карти , змусити зняти ліміти на операції по платіжній картці, відключити перевірку коду безпеки картки CVV2 або перерахувати кошти на картку шахраїв. Слід пам'ятати, що ніколи, нікому і ні за яких обставин не можна повідомляти термін дії платіжної картки і тризначний код безпеки CVV2, а також код підтвердження операції з банківського SMS-повідомлення.

Висновки. Багато людей на жаль, думають що в інтернеті заробити гроші без вкладень можна легко і просто, але при пошуку способів заробити грошей, часто потрапляють на шахраїв або шахрайський проект, а способів того, як розвести і вкрасти гроші, дуже багато, чорних схем заробітку, сірі і білі схеми є, але чорних більше. Заробити гроші в інтернеті можна, без вкладень, просто треба знати де.

УДК 343.1 + 004

МАНЖАЙ ОЛЕКСАНДР ВОЛОДИМИРОВИЧ

кандидат юридичних наук, доцент,

завідувач кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ОРГАНАМИ ТА ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Згідно з Інструкцією із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису, затвердженої наказом МВС України від 18.12.2018 р. № 1026 безпілотний літальний апарат (БпЛА) – це повітряне судно, призначене для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюються за допомогою спеціальної станції керування, що розташована поза повітряним судном. БпЛА можуть бути обладнані системами (однією або декількома) фото- і відеозапису