Олексюк Роман Анатолійович
слухач магістратури НАВС

Науковий керівник:
Школьніков Владислав Ігорович
доктор філософії, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ №1 НАВС, капітан поліції

ВІШИНГ: СУЧАСНА ЗАГРОЗА В МЕРЕЖІ ІНТЕРНЕТ

В сучасному цифровому світі інтернет-шахраї знаходять все більш винахідливі та складні способи обману. Однією з таких загроз є вішинг – вид інтернет-шахрайства, спрямований на отримання особистих даних та фінансових ресурсів користувачів. У цьому рефераті розглянемо основні аспекти вішингу, його наслідки та способи захисту від цієї загрози.

Вішинг – це форма інтернет-шахрайства, при якій шахраї використовують різні методи обману, щоб отримати доступ до особистих даних, банківських реквізитів та інших конфіденційних інформаційних ресурсів користувачів. Найчастіше вішинг відбувається через електронні листи, повідомлення в соціальних мережах, телефонні дзвінки тощо.

Типи вішингу:

- Фішинг – вішинг, який використовує електронні листи, які виглядають як листи від відомих компаній або установ, з метою викликати у користувача довіру та отримати від нього особисті дані.
- Веб-сайтовий вішинг – шахраї створюють фальшиві веб-сайти, що схожі на офіційні, для збору конфіденційних даних.
- СМС-вішинг – використання текстових повідомлень для введення користувача в оману та отримання від нього особистих даних.

Наслідки вішингу можуть бути дуже серйозними. Це може включати втрату фінансових коштів через шахрайство, втрату особистих даних, які можуть бути використані для ідентифікаційної крадіжки або шахрайства в мережі.

Способи захисту від вішингу:

- Ретельно перевіряйте джерела листів, повідомлень та веб-сайтів перед тим, як надавати будь-які особисті дані.
- Не відкривайте посилання або вкладення в сумнівних повідомленнях.
- Використовуйте надійне антивірусне програмне забезпечення та оновлюйте його регулярно.
- Ніколи не передавайте особисті дані через телефонні дзвінки або текстові повідомлення від невідомих джерел.

Вішинг є серйозною загрозою для користувачів інтернету, але з правильними заходами захисту можна уникнути попадання у пастку шахраїв. Освіта та свідоме використання інтернет-ресурсів є ключовими в боротьбі з цією формою кіберзлочинності.

Панченко Євгеній Вікторович
начальник 4-го управління Департаменту кіберполіції Національної поліції України, старший науковий співробітник аналітичного відділу (Центр кримінальної аналітики) Національної академії внутрішніх справ

Овсянюк Дмитро Іванович
начальник аналітичного відділу (Центр кримінальної аналітики) Національної академії внутрішніх справ

АНАЛІЗ КЛАСТЕРІВ ТА АДРЕС ГАМАНЦІВ ВІРТУАЛЬНИХ АКТИВІВ (КРИПТОВАЛЮТИ) ДЛЯ ЗБОРУ КОШТІВ НА ДОПОМОГУ РОСІЙСЬКІЙ АРМІЇ ТА ІНШИМ НЗФ

Повномасштабна війна в Україні триває більше двох років, рішучі та результативні зусилля українських військових перегорнули сторінку історії, наповнивши її перемогами та звільнивши велику частину територій України (Київську, Чернігівську, Сумську, Миколаївську, Харківську області та частину Херсонської області), що в свою чергу зосередило епіцентр активних бойових дій на Донецьку, Луганську та частину окупованої Запорізької, Херсонської області та АРК Крим, де російські війська супроводжуючись різними незаконними збройними формуваннями, зокрема ПВК «Вагнер» і підбадьорюючись пропагандою російських дезінформаційних кампаній продовжують свою агресію проти України.

В той же час, з публікацій української розвідки та міжнародних партнерів стає зрозуміло, що існує велика кількість невирішених питань всередині російської армії, що супроводжується неякісним забезпеченням, зменшенням постачань, відсутністю системних підходів до організації зв’язку та навчання тощо. Ряд російських волонтерських груп та їхніх прихильників намагаються виправити ситуацію, в тому числі використовуючи соціальні мережі, зокрема Telegram та VK для збору коштів на військові закупівлі, розвиток БПЛА та радіозв’язку тощо, збираючи пожертви, у тому числі у віртуальних активах (криптовалюті) на закупівлю товарів та компонентів.