УДК 343.72:004.773+578.834.1

Олексій Михайлович РВАЧОВ,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

Вікторія Олександрівна КОВТУН,
курсантка 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

СУЧАСНІ КІБЕРШАХРАЙСТВА ЩОДО ПРОТИЗАКОННОГО ЗАВОЛОДІННЯ КОШТАМИ З БАНКІВСЬКИХ РАХУНКІВ ГРОМАДЯН

До правопорушень у сфері використання інформаційних технологій можна віднести кібершахрайства, які зловмисники вчиняють з метою:

1. Крадіжки:

— особистих даних користувачів (наприклад, для отримання кредитів, створення фейкових акаунтів);
— логінів та паролів доступу до сайтів (наприклад, для розсилки спаму, шантажування);
— реквізитів банківських платіжних карток (кардінг);
— змісту листування;
— фотографій та відеозаписів приватного характеру;
— тощо.

2. Незаконного заволодіння коштами користувача через:

1) фейкові вебсайти:

— інтернет-магазини;
— поповнення рахунків мобільних телефонів;
— переказ грошей;
— участь у розіграші товарів;

2) шахрайські оголошення про продаж товарів та послуг в мережі Інтернет;

3) тощо [1].

Найчастіше для ошукування громадян кібершахраї використовують методи соціальної інженерії та інформаційні приводи, такі як, наприклад, пандемія гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2.

Найбільш популярною схемою впливу на особу, що використовується в соціальній інженерії, є схема білоруського психолога та соціолога В. П. Шейнова, яка полягає у таких кроках: 1) формування цілі впливу на об'єкт; 2) пошук інформації про об'єкт впливу; 3) виявлення найбільш зручних цілей впливу; 4) атракція – створення найбільш сприятливих умов для впливу на об'єкт; 5) примус до потрібної дії; 6) необхідний результат [2, с. 13].

До основних способів застосування соціальної інженерії можна віднести: фішинг; вішинг; фармінг; попередження про шкідливе програмне забезпечення на персональному пристрої користувача; «Quid pro quo»; «дорожне яблуко»; зворотна соціальна інженерія; претекстинг [3].

Одним із прикладів сучасних способів вчинення кібершахрайств є надсилання зловмисниками на адресу користувачу електронного листа із його логіном та паролем від якогось інформаційного ресурсу. Такі листи можуть в автоматичному режимі розсилати спеціально створені зловмисниками програми, які аналізують викрадені бази даних, знаходять там адреси електронних скриньок користувачів, які вони зазначали під час реєстрації на ресурсі, базу даних якого викрали. У листі зловмисники намагаються шантажувати користувача розповсюдженням його конфіденційної інформації, яка стала їм начебто відома через наявність у шахраїв логіну та пароля користувача, які він, скоріш за все, міг використовувати під час реєстрації на інших інтернет-ресурсах.

Також продовжується розсилка фішингових електронних листів та повідомлень від реально існуючих популярних організацій чи установ, про які нещодавно активно писали у ЗМІ, чи клієнтом яких з великою ймовірністю може бути отримувач повідомлення. Наприклад, у якості відправника листа може бути зазначена банківська установа, правоохоронний орган, національна чи міжнародна організація охорони здоров'я тощо. Зазвичай додатком (вкладенням) до такого листа є якийсь текстовий документ, із яким отримувач, на дії якого вплинули, використовуючи методи соціального інжинірингу, повинен обов'язково ознайомитися. Під час відкриття користувачем такого файлу відбувається зараження

його персонального пристрою шкідливим програмним забезпеченням, яке бере під свій контроль роботу цього пристрою та негласно збирає і передає шахраям конфіденційні дані користувача: логіни, паролі, номера банківських карток, усі нажаті клавіші на пристрої, зображення його екрану тощо.

Через пандемію COVID-19 шахраї почали використовувати цей інформаційний привід для розсилки повідомлень із пропозицією взяти участь у онлайн-опитувані, що начебто проводить іноземна медична організація з метою вивчення стану поширення хвороби на певній території. Учаснику пропонується отримати чималу суму коштів за участь в анкетуванні. Для того щоб отримати кошти користувач повинен надати дані своєї банківської платіжної картки. При цьому шахраї видурюють у довірливих громадян не тільки номер картки, термін її дій, але й CVV/CVC код, що дозволяє їм здійснювати несанкціоновані перекази з банківського рахунку ошуканої особи.

Також зловмисники використали повідомлення від органів державної влади про виплати 1000 гривень пенсіонерам, які отримують пенсію меншу за 5 тис. грн., а також іншим визначеним категоріям громадян. Громадяни почали масово отримувати на свої мобільні телефони SMS-повідомлення начебто від Національного банку, інших банківських установ, Пенсійного фонду про необхідність уточнення реквізитів отримувачів цих виплат. Під час того як отримувачі повідомлень телефонували за номерами телефонів, зазначеними у повідомленнях, вони розмовляли, самі того не розуміючи, із шахраями, які заволодівали їх особистими даними та інформацією про наявні в них банківські картки та рахунки [4].

Останні декілька років набули популярності шахрайські дії, пов'язані з використанням шахраями популярних вебсайтів із продажу товарів та надання послуг, наприклад, olx.ua. Шахрайська схема полягає в тому, що шахраї розміщують оголошення про продаж за привабливо низькою ціною популярного товару. Під час спілкування із потенційним покупцем шахраї пропонують йому продовжити спілкування в іншому, більш зручному для них, месенджері, наприклад, Viber, Telegram, WhatsApp тощо. Під час спілкування з покупцем через месенджер шахраї пропонують оформити придбання товару через сервіс маркетплейсу (сайту оголошень) та відправляють покупцю гіперпосилання на відповідну сторінку. Але насправді покупець потрапляє на фішинговий вебсайт, який копіює реально існуючий офіційний вебсайт, доменне ім'я якого

або відрізняється декількома символами від реального, або частково містить його у своїй адресі. Покупець переказує через підроблений вебсайт свої кошти, якими протизаконно заволодівають зловмисники [5].

Також останні декілька років шахраї незаконно отримують доступ до SIM-карток операторів мобільного (рухомого) зв'язку з номерами телефонів реально існуючих громадян, які використовувалися для реєстрації на вебсайтах, додатках для смартфонів та дистанційного банківського обслуговування.

Для отримання SIM-картки з номером мобільного телефону реальної існуючої людини, зловмисники безпосередньо звертаються до офісів з обслуговування клієнтів операторів мобільного зв'язку та повідомляють про нібито загублену ними SIM-картку та просять видати їм нову. Для того, щоб здійснити цю операцію, представник оператора просить надати інформацію про вхідні чи вихідні дзвінки та суму останнього поповнення рахунку власником загубленої SIM-картки. Щоб заволодіти номером мобільного телефону, зловмисники кілька разів поспіль телефонують жертві з різних телефонів та іноді поповнюють рахунок на невелику суму. Відповідно, маючи необхідну інформацію, шахраї передають її оператору та отримують SIM-картку з прив'язаним до неї номером телефону жертви.

Також ще один спосіб отримання SIM-картки з номером телефону жертви полягає в тому, що шахраї купують спеціальні SIM-картки, що офіційно продають оператори мобільного телефону для заміни старих SIM-карток на нові для використанням їх у нових смартфонах, які підтримують стандарт зв'язку 4G або в яких може використовуватися тільки nanoSIM-картка. У такому випадку шахраї телефонують жертві та представляються їй працівниками оператора мобільного зв'язку, пропонують, наприклад, перейти на більш привабливі тарифи, для чого користувач повинен назвати їм код із SMS, яка насправді надсилається абоненту для підтвердження заміни його SIM-картки новою. Після того, як жертва передає код із отриманого нею SMS, її SIM-картка блокується, мобільний пристрій перестає реєструватися у мобільній мережі, отримувати та надсилати SMS, здійснювати телефонні дзвінки, користуватися мобільним інтернетом стає неможливим. Шахраї ж отримують доступ до номера телефону потерпілого та, використовуючи сервіси відновлення забутих паролів у соціальних комп'ютерних

мережах, банківських установ тощо, отримують доступ до ресурсів, де був зареєстрований власник номеру [6].

Фахівці у сфері кібербезпеки та фінансової грамотності наголошують, що користувачі сучасних інформаційних технологій повинні бути пильним, щоб не стати жертвами кібершахраїв та не втратити свої кошти і конфіденційну інформацію.

Список бібліографічних посилань

1. Зуб Л. В., Рвачов О. М. Сучасні загрози сімейній онлайн безпеці: класифікація та профілактика виникнення // Актуальні питання протидії кіберзлочинності та торгівлі людьми : зб. матеріалів Всеукр. наук.-практ. конф. (м. Харків, 23 листоп. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків, 2018. С. 149–154. URL: http://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/45.pdf (дата звернення: 10.05.2020).
2. Кузнецов М. В., Симдянов И. В. Социальная инженерия и социальные хакеры. СПб. : БХВ-Петербург, 2007. 368 с.
3. Демчук П. В. Соціальна інженерія: виклики та перспективи боротьби в українському контексті: есе з права ІТ // Українське право : сайт. 01.11.2017. URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain/ (дата звернення: 10.05.2020).
4. Шахраї розсилають смс-повідомлення про нібито отриману 1000 грн від НБУ // Цензор.НЕТ : сайт. 26.03.2020. URL: https://censor.net.ua/ua/news/3184703/shahrayi_rozsylayut_smspovidomlennya_pro_nibyto_otrymanu_1000_grn_vid_nbu (дата звернення: 10.05.2020).
5. Поради продавцям і покупцям. Правила безпечних покупок // OLX : сайт. URL: https://help.olx.ua/hc/uk/articles/360010019480 (дата звернення: 10.05.2020).
6. Як запобігти крадіжці SIM-карти та грошей // Obozrevatel : сайт. URL: https://www.obozrevatel.com/story/krazha-sim-karty/ (дата звернення: 10.05.2020).

Одержано 11.05.2020