Ковальчук А. Ю.,
доктор юридичних наук, професор, начальник відділу дослідження проблем протидії кіберзлочинності та загрозам інформаційній безпеці МНДЦ при РНБО України
(м. Київ, Україна)

СОЦІАЛЬНИЙ ХАКІНГ ЯК СКЛАДОВА КІБЕРАТАКИ: МЕТОДИ ВЧИНЕННЯ І ЗАХОДИ ПРОТИДІЇ

В останні роки в усьому світі зберігається тенденція щодо збільшення кількості кіберзлочинів, які спрямовані на отримання фінансового прибутку.

У нових кримінальних інцидентах спостерігається зміна тактики дій злочинців [1;2]. Вони атакують різні об'єкти критичної інфраструктури залучаючи до своїх атак як новітні технологій так й інші соціотехнологічні засоби (соціальна інженерія та соціальне програмування). Також трендом початку 2025 року стає поширення залучення великих мовних моделей для просування власних інтересів і вчинення кібератак та розширення методології соціальної інженерії та соціального програмування. Соціальна інженерія є багатогранним і складним способом отримання конфіденційної інформації від користувачів із застосуванням методів переконання і технологічних засобів. Поняття соціальної інженерії було введено Кевіном Митником [3] і досить часто згадується в низці статей та доповідей з тематики безпеки мереж та інформації [4]. Статистика демонструє, що велика кількість людей ставиться до використання власної конфіденційної інформації недостатньо уважно. Для прикладу можна розглянути вибір складності паролів, обставини доступу до онлайн-рахунку в банку тощо. Також яскравим прикладом є необережність при вході в соціальні мережі. Поняття паролю і таємного (секретного) запитання здається тривіальним для більшості користувачів, хоча недооцінювати їх значення не можна.

При використанні різноманітних технік соціальної інженерії зазвичай відсутня потреба у глибоких знаннях технічних галузей та інформаційних технологій, проте при наявності таких знань у зловмисника вірогідність несанкціонованого доступу до інформаційних ресурсів значно підвищується.

Кримінальне маніпулювання може застосовуватися під час низки корисливих і насильницьких злочинів. Серед корисливих злочинів, що здійснюються з використанням такого впливу на особистість, виділяється шахрайство, різноманітні види якого сьогодні досить поширені в мережі Інтернет.

Кримінальне маніпулювання здійснюється в комунікативному процесі під час взаємодії злочинця та жертви з використанням комплексу методів і прийомів, у тому числі сучасних психотехнологій. О. В. Кравченко визначає кримінальну маніпуляцію як процес цілеспрямованого використання різних специфічних

способів і засобів зміни (модифікації) поведінки жертви злочину, її мети, бажань, намірів, відносин, установок, психічних станів та інших її психологічних характеристик в інтересах шахрая, які могли б не відбутися, якби потерпілий знав у достатньому обсязі дані, що характеризують ситуацію, зокрема те, які засоби застосовано щодо нього чи з якою метою їх використано [5]. Психологічною передумовою застосування методів соціальної інженерії є така особливість людської психіки, як когнітивні упередження. Через це надійність комп'ютерної системи є не вищою, ніж надійність її оператора. Зловмисники проникають навіть у добре спроектовані, захищені комп'ютерні системи, скориставшись неуважністю довірених користувачів або умисно вводячи їх в оману (наприклад, відрекомендувавшись системним адміністратором або вищестоящим посадовцем). Обман (повідомлення потерпілому неправдивих відомостей або приховування певних обставин) чи зловживання довірою (недобросовісне використання довіри потерпілого) під час шахрайства застосовує винна особа для того, щоб викликати в потерпілого впевненість у вигідності чи обов'язковості передачі їй майна або права на нього. Обов'язковою ознакою шахрайства є добровільне передавання потерпілим майна чи права на нього.

Обман під час шахрайства – це повідомлення явно помилкових даних або приховування, замовчування інформації про факти чи обставини, повідомити про які було необхідно, спрямовані на введення потерпілого в оману або на підтримання помилки особи з метою заволодіння чужим майном, і які призвели до такого стану потерпілого [5].

В мережі Інтернет для отримання несанкціонованого доступу зловмисники використовують різноманітні типи кібератак, наприклад, шляхом уведення шкідливого програмного забезпечення (ШПЗ) у код вебсайту або пересилання різноманітних видів ШПЗ (вірусів, троянів тощо) до комп'ютерної системи потерпілого. Атаки такого виду перешкоджають керуванню пошкодженим продуктом або його налагодженню. Що ж стосується соціальної інженерії, то цей тип атак спрямований не безпосередньо на комп'ютерну систему, а на її користувачів — «найслабшу ланку», і шляхом обходу інфраструктури, призначеної для захисту від ШПЗ, він дозволяє досягти тих же результатів, що й інші види кібератак. Оскільки такі прийоми значно складніше виявити чи запобігти їм, цей напрям атак є набагато ефективнішим за інші.

Основна тактика соціальної інженерії полягають у психологічних методах, за допомогою яких стає можливим переконати користувача розкрити інформацію особистого характеру (паролі, номери кредитних карток тощо). В основі методів використання соціальної інженерії – маніпуляція людськими страхами, зацікавленістю або довірою. Жертвою соціальної інженерії можна стати як під час особистого спілкування, так і по телефону або через цифрові гаджети. «Кіберзлочинці використовують такі способи експлуатації людського фактору як цікавість і довіра, – які призводять до того, що люди з добрими намірами потрапляють у руки зловмисників. Це може статися у формі замаскованої URL-адреси або, здавалося б, нешкідливого додатку в

електронному листі. Але все, що потрібно, – це один клік, і негайно почнеться поширення шкідливої програми», – пояснює стратег із кібербезпеки Аденікі Косґроув виданню Forbes [6].

Висновки. Дослідження показують, що людям притаманні деякі поведінкові нахили, які можна використовувати для обережного маніпулювання. Багато з найбільш шкідливих зламів систем безпеки відбуваються і відбуватимуться завдяки соціальній інженерії, а не електронному злому. Наступне десятиліття соціальна інженерія сама по собі становитиме найвищу загрозу інформаційній безпеці.

Список використаних джерел:

1. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 URL: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
2. Internet crime report 2021 URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
3. Біленчук П.Д., Гуцалюк М.В., Кравчук О.В., Козир М.В. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти: Монографія / За заг. Ред. П.Д. Біленчука. – К.: Наука і життя, 2008. 291 с.
4. Matthew J Duffy, Social Engineering / UWP Computer Science and Software Engineering Technical Report, Volume 12, 2011.
5. Кравченко О. В. Психологічні особливості шахрайства: автореф. дис. на здобуття наук. ступеня канд. психол. наук : спец. 19.00.06 «Юридична психологія» / О. В. Кравченко. – Х., 2005. – 20 с.
6. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті URL: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html .