УДК 004.056.5

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ,

http://orcid.org/0000–0003–3381–3350

ДЕЯКІ ОСОБЛИВОСТІ АТАК ХАКЕРІВ ІЗ ВИКОРИСТАННЯМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія - це способи маніпулювання людьми з метою отримання від них конфіденційної інформації. Ці дії хакери роблять із єдиною метою — заволодіти особистими даними користувачів. Інформація, яку шукають хакери, може бути різною, але найчастіше це банківські реквізити, а також паролі від облікових записів. Крім того, кіберзлочинці можуть спробувати отримати доступ до комп'ютера жертви, щоб встановити там шкідливе програмне забезпечення, яке допомагає витягувати будь-яку інформацію. І тут хакери використовують різноманітний арсенал соціальної інженерії, адже значно легше отримати від людини бажане (персональні дані), завоювавши його довіру. Це значно зручніший шлях, ніж прямий злом чийогось облікового запису: використовувати слабкості користувачів набагато простіше, ніж намагатися знайти вразливість сервісу або програмного забезпечення.

Найчастіше атаки з використанням засобів соціальної інженерії відбуваються у два етапи. Спочатку хакери досліджують ймовірну жертву, щоб зібрати необхідну довідкову інформацію. Саме на цьому етапі хакер намагається здобути довіру жертви. А після успішних спроб налагодити «добрі» стосунки кіберзлочинець, використовуючи різні хитрощі, витягує з жертви конфіденційну інформацію (наприклад, паролі та IP-адреси) [1].

Відомо більше десяти видів атак з використанням соціальної інженерії, а якщо врахувати комбіновані способи, їх кількість налічує вже кілька десятків.

Фішинг (Phishing). Ці атаки активно експлуатують людський чинник для збору облікових даних або поширення шкідливих програм. Можна сказати, що фішинг - це шахрайське використання електронних комунікацій для обману та отримання користі від користувачів. Найчастіше за допомогою фішингових атак хакери намагаються отримати таку конфіденційну інформацію , як логіни та паролі, дані кредитних карток, мережеві облікові дані. Також фішингова атака може бути спланована таким чином, що після переходу на підроблений сайт у жертви виникнуть інші неприємності: наприклад, на комп'ютер встановиться шкідливе шпигунське програмне забезпечення або зависатиме система через атаку програми-вимагача. У ряді випадків хакери задовольняються отриманням інформації про кредитну картку жертви або інші особисті дані для отримання фінансової вигоди. Але буває, що фішингові електронні листи надсилаються для отримання реєстраційної інформації співробітника або інших даних для подальшої розширеної атаки на конкретну компанію.

Цільовий фішинг (Spear Phishing). Такі атаки схожі на звичайний фішинг, проте націлені вони на конкретну людину чи організацію. Тому спочатку хакери збирають докладну інформацію про свої цілі, щоб потім надсилати електронні листи, які виглядають максимально правдоподібними. Людина часто немає і думки, що фішинговий лист надійшов з ненадійного джерела. Цільовий фішинг можна назвати більш просунутою версією звичайного, оскільки він вимагає набагато солідніші підготовки. З цієї причини захиститись від такої атаки звичайними технічними засобами вкрай складно. Крім того, особа, яка піддається цільовому фішингу, в більшості випадків не є реальною метою злочинців — їх кінцевою метою зазвичай стає корпоративна мережева інфраструктура, отримавши контроль над якою, хакери отримають із цього фінансову вигоду.

Голосовий фішинг (Vishing, Voice Phishing). У цьому випадку хакери використовують телефон для збирання особистої та фінансової інформації жертви. Наприклад, хакер може представитися співробітником банку або страхової компанії і під приводом реклами нових послуг поступово вивідувати

особисті дані співрозмовника. Так, "вішери" можуть заставати своїх жертв зненацька, пропонуючи їм отримати кредит на вкрай вигідних умовах. А оскільки такі послуги часто пов'язані з розголошенням особистої фінансової інформації, то, якщо хакер зможе переконати жертву в законності своєї пропозиції, людина може навіть не запідозрити каверзи і передати злочинцеві конфіденційну інформацію.

Смішинг (Smishing, SMS-фішинг). Для цього виду атак фішингу задіяні мобільні пристрої. Жертві надходить повідомлення нібито з номера банку. У повідомленні зазвичай міститься деяка лякаюча інформація (див. розділ Scareware нижче), а потім пропонується вирішення проблеми. Класичний приклад: з особового рахунку жертви нібито здійснено нецільове списання коштів, тому людині пропонується перейти за посиланням на сторінку банку (зрозуміло, підроблену) або зателефонувати за вказаним номером телефону (теж контрольованому шахраями). Також людям надходять повідомлення з проханням допомогти постраждалим від будь-якого стихійного лиха, але щоб допомогти, потрібно залишити свої особисті дані. Особливо хитрі хакери можуть таким чином місяцями використовувати своїх жертв, регулярно знімаючи невеликі суми, щоб не насторожувати людей.

«Китобійний» фішинг (Whale Phishing). Це фішингова атака, орієнтована безпосередньо на топ-менеджера великої компанії. Тому вона і називається «китобійною» [2], адже жертва оцінюється високо, а вкрадена інформація буде набагато ціннішою, ніж та, яку можуть запропонувати шахраям звичайні співробітники компаній. А оскільки жертвами в даному випадку обираються високопосадовці, злочинці діють відповідним чином: наприклад, надсилають повідомлення юридичного характеру або пропонують обговорити серйозні фінансові питання.

Клон-фішинг Clone Phishing). Принцип цієї фішингової атаки полягає в тому, що хакер відправляє підроблений електронний лист, замаскований під звичайне, причому адреса, з якої був відправлений лист, дуже схожий на один з тих, які використовують відомі та надійні джерела. Тобто фішингові електронні

листи виглядають так, ніби їх надіслав ваш банк чи провайдер послуг, і його співробітники просять надати вашу особисту інформацію. Таким чином, хакери копіюють форму корпоративного електронного листа, створюючи майже ідентичний зразок: тільки такий лист відправляється не з справжньої, а з схожої адреси. Тіло листа виглядає так само, як і в листах, які користувач вже отримував від цієї організації, проте посилання в листі замінюються на шкідливі. Крім того, винахідливі злочинці можуть навіть пояснити жертві, чому вона знову отримує «те саме повідомлення». Фактично такі листи мають на меті єдину мету: «соціальні хакери» намагаються змусити одержувача розкрити особисту або фінансову інформацію шляхом натискання на посилання в листі, в результаті чого користувач перенаправляється на зовні схожий, але контрольований злочинцями сайт, призначений для крадіжки особистої інформації.

Scareware (пугалка). Суть цього типу атак полягає в тому, що жертву лякають (найчастіше спливаючими вікнами при відвідуванні зламаних шахраями сайтів), змушуючи думати, що її комп'ютер заражений шкідливим програмним забезпеченням (ПЗ), або має випадково завантажений нелегальний контент. Через деякий час, коли хакер розуміє, що жертва дозріла, він пропонує вирішення цієї фіктивної проблеми. Однак насправді та програма, що пропонується жертві під виглядом антивірусу, є шкідливим ПЗ, метою якого є розкрадання особистої інформації користувача. Таким чином, творці « пугалок » використовують технологію навіювання, викликаючи страх користувача та підштовхуючи його до встановлення підробленого антивірусного програмного забезпечення.

Baiting (приманка). Дуже оригінальний метод соціальної інженерії, коли розрахунок робиться однією з найпоширеніших людських вад - цікавість. Суть приманки в тому, що хакер навмисно залишає заражені шкідливим програмним забезпеченням (наприклад, USB-накопичувачі) у місцях, де їх обов'язково знайдуть (наприклад, у курилці офісної будівлі). Жертва заковтує цю нехитру наживку і вставляє флешку комп'ютер, внаслідок чого відбувається автоматичне встановлення шкідливих програм у систему. Ще один вид наживок поширюється

через Інтернет. Потенційним жертвам пропонується приваблива реклама, яка насправді веде на шкідливі сайти або спонукає користувачів завантажувати заражений шкідливим програмним забезпеченням — найчастіше, зрозуміло, «безкоштовний». Крім того, хакери нерідко комбінують приманки зі Scareware - атаками, тільки цього разу « лякалки » справжні, адже комп'ютер уже заражений.

Water-Holing («водопой»). Назва повністю відображає суть атаки, тільки «вода» тут отруєна. Використовуючи вразливості мереж, хакер намагається скомпрометувати певну групу людей, заражаючи сайти, які вони відвідують і яким довіряють. Об'єктами атак типу «водопою» нерідко стають популярні сайти, які називають «цільовою групою» (target group). Своїх жертв кіберзлочинці, які практикують Water holing (інша назва: Watering hole), називають «цільовим видобутком» (target prey), і найчастіше в ролі такого видобутку виступають співробітники державних установ чи великих організацій. Хакери вивчають уразливості сайтів «цільової групи» і впроваджують туди шкідливе ПЗ, зазвичай заховане JavaScript або прямо в HTML коді. Цей шкідливий код перенаправляє «видобуток» із сайтів цільової групи на інший, де встановлено шкідливе програмне забезпечення або реклама. Тепер віруси готові заражати комп'ютери, щойно жертви заходитимуть на скомпрометовані сайти.

Pretexting attack (атака з прийменником). Суть атаки полягає в тому, що одна сторона просто бреше іншою, щоб отримати доступ до привілейованих даних. Шахрайство часто ініціюється несумлінним співробітником, який вдає, що йому потрібна конфіденційна інформація від жертви для виконання важливого завдання. Жодного злому — чистий психологічний вплив, який виглядає дуже природно.

Quid pro quo (лат. «послуга за послугу»). Така атака зазвичай виконується шахраями, які не мають у своєму арсеналі просунутих інструментів злому, проте проводять попереднє дослідження цілей. Використовуючи цей вид атак, зловмисник вдає, що надає жертві важливу послугу. Наприклад, хакер знаходить когось із високими привілеями доступу до мережі та дзвонить йому по телефону, представляючись співробітником служби технічної підтримки компанії. При

успішних переговорах та злагоді жертви на «допомогу» у вирішенні нібито виявлених проблем, хакер починає керувати жертвою, змушуючи її вчиняти певні дії. Ці дії в результаті призводять до запуску шкідливого ПЗ в систему або до крадіжки реєстраційних даних.

Honey Trap, Honey Pot («медова пастка», «горщик меду»). Хакер знайомиться з жертвою і вдає, що відчуває до неї певний інтерес (наприклад, романтичний або сексуальний потяг). Поступово зав'язуються віртуальні «відносини», які жертва починає сприймати всерйоз. А чарівний кіберзлочинець, не гаючи часу даремно, поступово збирає конфіденційну інформацію, яка потім може бути використана, наприклад, для злому акаунтів у соцмережах або скриньки електронної пошти. Також хакер може отримати від довірливої жертви віддалений доступ до її комп'ютера.

Tailgating або Piggyback («задні двері», «катання на спині»). Ще один оригінальний прийом із арсеналу фахівців із соціальної інженерії, який чимось схожий на попередній. В даному випадку злочинець входить в приміщення, що охороняється, слідуючи за кимось з картою доступу. Зрозуміло, хакер вже є "другом" співробітника з привілейованим доступом і проходить за ним у зону зборони.

Rogue Attack (шахрайська атака). Цей спосіб є різновидом Scareware атак. На комп'ютер жертви під приводом безпеки встановлюється шкідливе ПЗ, а хакер переконує жертву, що це програмне забезпечення є цілком законним і безпечним. Встановлена програма створює спливні вікна та оповіщення, які радять користувачеві завантажити нове «безпечне програмне забезпечення». Спливаючі вікна нерідко показують користувачеві кілька варіантів угоди (з різними сценаріями). Однак різниці немає: натиснувши «так» на будь-який із цих варіантів, користувач завантажує на свій комп'ютер небезпечну програму.

Висновки. Проте, існує низка досить надійних заходів, які можна використовувати для протидії маніпуляціям хакерів. Насамперед це стосується навчання та обізнаності. Необхідно навчати співробітників організацій та звичайних користувачів розпізнаванню ознак соціальної інженерії. Також

важливо бути обережними при наданні особистої інформації. Не менш важливо звертати увагу на автентифікацію. При отриманні запитів на надання інформації або виконання певних дій необхідно переконатись у справжності джерела запиту. Не варто надавати особисті дані через електронні листи чи телефонні дзвінки третім особам. Кожен користувач мережі завжди має бути гранично обережним у соціальних мережах. І не повинен розголошувати персональну інформацію, яку можуть використовувати зловмисники для маніпуляції. Крім того, фахівці радять [3]:

- обмежити доступ до конфіденційної інформації, надаючи його лише необхідним співробітникам та користувачам;
- використовувати двофакторну автентифікацію для посилення захисту облікових записів;
- встановити суворі правила керування доступом для всіх систем та додатків;
- регулярно оновлювати безпекову політику;
- знайомити співробітників з новими хитрощами хакерів, які використовують соціальну інженерію;
- впровадити системи моніторингу активності, щоб швидко виявляти підозрілу активність й запобігати витоку даних.

Безумовно, стовідсотково захищених систем та мереж немає. Проте, виконання вищеперелічених рекомендацій дозволить мінімізувати ризик вдалої хакерської атаки.

Список використаних джерел:

1. Соціальна інженерія та її використання у кібератаках – стаття від «Cisco, мережна академія» – Education.ua. *Освіта в Україні. Усі навчальні заклади – Education.ua*. URL: https://www.education.ua/blog/48050/ (дата звернення: 21.11.2023).

2. Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme. *Department of Justice | Homepage | United States Department of Justice*. URL: https://www.justice.gov/usao-

sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business (date of access: 21.11.2023).

3. Соціальна інженерія - Послуги з тестування та консультування персоналу - Кібербезпека - Kiss Software. *kiss.software*. URL: https://kiss.software/ua/what-we-do-details/social-engineering (дата звернення: 21.11.2023).

УДК 004.8

СТРУКОВ ВОЛОДИМИР МИХАЙЛОВИЧ

кандидат технічних наук, доцент,

професор кафедри кібербезпеки та DATA-технологій

факультету №6 Харківського національного університету внутрішніх справ

ORCID ID: http://orcid.org/0000-0003-4722-3159;

УЗЛОВ ДМИТРО ЮРІЙОВИЧ

кандидат технічних наук,

в.о. декана факультету комп'ютерних наук Харківського національного університету ім. В.Н. Каразіна;

ORCID: https://orcid.org/0000-0003-3308-424X

ГНУСОВ ЮРІЙ ВАЛЕРІЙОВИЧ

кандидат технічних наук, доцент,

завідувач кафедри кібербезпеки та DATA-технологій факультету №6 Харківського національного університету внутрішніх справ;

ORCID ID: http://orcid.org/0000-0002-9017-9635;

ВЛАСОВ ОЛЕКСІЙ В'ЯЧЕСЛАВОВИЧ

начальник відділу цілодобової технічної та інформаційної підтримки УІАП ГУНП в Харківській області

ОГЛЯД НАЦІОНАЛЬНОЇ СТРАТЕГІЇ США У ГАЛУЗІ ШТУЧНОГО ІНТЕЛЕКТУ