Сучасні методи соціотехнічних атак

УДК 004.056.53(045)

Анна Корченко[1], Кирило Давиденко[2],

[1,2]Національний технічний університет «Дніпровська політехніка»,
[1]annakor@ukr.net, [2]kirilldavy@gmail.com

Стрімкий розвиток інформаційних технологій та зростаючий обмін даними через Інтернет відкривають нові можливості, але при цьому збільшують загрози для безпеки. Попит на цифрові послуги також породжує нові види кіберзлочинності, такі як шахрайство, крадіжка особистих даних і фішинг. Швидкий обмін даними в Інтернеті також збільшує ризики кібершпигунства, коли конфіденційна інформація може бути вкрадена або перехоплена.

Останнім часом спостерігається збільшення застосування соціального інжинірингу як ефективного методу кібератак. Оскільки людина є найбільш уразливим ланцюжком у системі кібербезпеки, кіберзлочинці активно використовують соціотехнічні методи. Розуміння цих методів дозволяє розробляти ефективні заходи захисту для користувачів і організацій.

Тому, аналіз сучасних методів соціотехнічних атак є ключовим елементом стратегії кібербезпеки, який допомагає забезпечити захист від неперервно зростаючих загроз та є актуальним науковим завданням, яке стоїть перед науковою спільнотою.

Згідно з провідними дослідженнями, серед найбільш поширених методів соціотехнічних атак можна виділити такі: фішинг, водопій, атака китобоя, під приводом, атаки приманка і послуга за послугу, голосовий фішинг, медова пастка, задні двері, смішинг, спір фішинг та інші. Однак в цих публікаціях не сформован повний опис характеристик, що визначають кожен з цих методів соціотехнічних атак.

Аналіз відповідних методів сприятиме більш глибокому розумінню різноманітних аспектів соціотехнічних атак і допоможе у розробці ефективних стратегій протидії їм.

Тому, на базі відомих досліджень [1-4] з подальшим їх узагальнюванням проведемо аналіз сучасних методів соціотехнічних атак (СМСА) за наступними критеріями:

1. За часовим аспектом СМСА поділяються на спонтанні (СП-атаки) та попереднього планування (ППЛ-атаки).

2. За галузевою афіліацією СМСА поділяються на атаки на корпоративний сектор (КС-атаки) та атаки на громадські установи (ГУ-атаки).

3. За взаємодією з політикою безпеки СМСА поділяються на постполітизаційні (ПП-методи) та деполітизаційні (ДП-методи) методи.

4. За ініціалізацією СМСА поділяються на умовні (УМ-атаки) та безумовні (БМ-атаки) атаки.

5. За типом звернення СМСА поділяються на аверсні (АВ-методи) і реверсні (РВ-методи).

6. За інструментарієм СМСА поділяються на програмні (ПМ-методи), апаратні (АМ-методи) та нетипові (НМ-методи) методи.

7. За порушенням характеристик безпеки СМСА поділяються на три типи: К-дієві, Ц-дієві та Д-дієві.

8. За ступенем важкості СМСА поділяються на прості (П-атаки), складні (С-атаки) та системні (СС-атаки).

9. За реляційними ознаками СМСА поділяються на чотири типи: мономономні (ММ-атаки), полімономні (ПМ-атаки), монополічні (МП-атаки) та поліполічні (ПП-атаки).

10. За типом атакованого джерела СМСА поділяються на чотири категорії: ЕК-джерельні (експерт), ЛГ-джерельні (легковажна особа), КН-джерельні (люди-контактери), ВП-джерельні (випадкова людина), а тип атакованого джерела визначається залежно від рівня інформованості особи, що піддається атаці.

11. За типом доступу до інформації СМСА поділяються на відкритого (ВК-доступу), умовно відкритого (УВ-доступу), конфіденційного (КН-доступу) та секретного (СК-доступу) доступу.

12. За дистанційністю СМСА поділяються на локальні (КТ- локальні, ПР-локальні, РМ-локальні, ЗД-локальні) та віддалені (Т-віддалені, МТ-віддалені, РП-віддалені).

13. За маніпулюванням СМСА поділяються на шість категорій, що включають риси людської натури: авторитетність (АВ-маніпулювання), прихильність (ПР-маніпулювання), взаємність (ВМ-маніпулювання), відповідальність (ВД-маніпулювання), соціальність (СЦ-маніпулювання) та обмеженість (ОБ-маніпулювання).

14. За типом соціотехніка СМСА поділяються на ті які виконуються хакерами (ХК-виконавчі), пенетрейшн-тестерами (ПТ-виконавчі), шпигунами (ШГ-виконавчі), злодіями ідентичності (ЗІ-виконавчі), незадоволеними співробітниками (НС-виконавчі), шахраями (ШХ-виконавчі), рекрутерами (РК-виконавчі), продавцями (ПР-виконавчі), з використанням віддалених комбінацій (ВК-виконавчі) та методи що націлені на конкретний сектор (СК-виконавчі), що ранжуються за специфікою діяльності і спрямовані на урядовців (УР-виконавчі), лікарів (ЛР-виконавчі), психологів (ПС-виконавчі), юристів (ЮР-виконавчі) тощо.

15. За масштабом СМСА поділяються на локальні (ЛК-атаки) та глобальні (ГБ-атаки) атаки.

Також, на базі запропонованого аналізу СМСА та набору критеріїв можна описати приклад здійснення соціотехнічної кібератаки.

Далі, приведемо загальний опис процесу звичайної соціотехнічної атаки, яка може мати свої унікальні особливості в залежності від цілей, методів і засобів зловмисника та включає наступні кроки:

Крок. 1. Дослідження цілі. Зловмисник починає з дослідження своєї цілі, будь то компанія, окрема особа або організація. Він збирає інформацію про цільову особу або організацію, таку як контактні дані, роль в організації, соціальні мережі тощо.

Крок. 2. Підготовка соціальної інженерії. Зловмисник розробляє стратегію впливу на цільову особу. Це може включати створення підроблених електронних

листів, створення фальшивих акаунтів у соціальних мережах або підготовку підроблених веб-сайтів.

Крок. 3. Виконання атаки. Зловмисник виконує заплановану атаку, яка може включати відправлення фішингових електронних листів з вимогою введення конфіденційної інформації, перехоплення даних або навіть використання соціальних інженерних методів для отримання доступу до системи.

Крок. 4. Експлуатація отриманої інформації. Після успішного здійснення атаки зловмисник може використовувати отриману інформацію для різних цілей, таких як крадіжка конфіденційних даних, використання цільових систем для здійснення подальших атак або навіть вимагання викупу за повернення доступу до скомпрометованих систем.

Крок. 5. Приховання слідів. На останньому етапі зловмисник може намагатися приховати свої сліди, щоб уникнути виявлення та відповідальності за атаку.

Запропонований аналіз СМСА за рахунок розширення існуючих класифікацій відповідних методів та додавання нових критеріїв, як от часовий аспект, галузева афіліація, взаємодія з політикою безпеки, дистанційність, ініціалізація, інструментарій, маніпулювання, порушення характеристик, реляційні ознаки, ступінь важкості, тип атакованого джерела, тип доступу, тип звернення, тип соціотехніка, масштаб, дозволить враховувати зазначені критерії при виборі відповідних засобів протидії соціотехнічним атакам та розробляти ефективні заходи захисту для користувачів та організацій, що є важливою складовою стратегії кібербезпеки для забезпечення захисту від постійно зростаючих кіберзагроз.

1. Класифікація методів соціального інжинірингу / О.Г. Корченко, Є.В. Паціра,Д.А. Горніцька // Захист інформації. – 2007. – №4 (36). – С.37-45.
2. О. Г. Корченко, Д. А. Горніцька, та А. Ю. Гололобов, «Розширена класифікація методів соціального інжинірингу», Безпека інформації, т. 20, № 2, с. 197-205, 2014.
3. Д. А. Горницька, А. Г. Корченко, В. П. Харченко, «Система соціально-технічних атак в інформаційному середовищі», II Міжнародна науково-практична конференція «Проблеми економіки та менеджменту на залізничному транспорті», Київ, 2007, с. 137-138.
4. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.