НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»
УДК 004.75, 003.26

«До захисту допущено»
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2024 р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-професійною програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Аналіз стійкості протоколів консенсусу Proof-of-history і Proof-of-authority до атак централізації та їх застосування в задачі оцінки якості ІОС»**

Виконав:
студент II курсу, групи ФІ-22мн
Бондаренко Андрій Андрійович _____

Керівник:
професор, д.т.н., с.н.с.
Кудін Антон Михайлович _____

Рецензент:
доцент, к.т.н
Стьопочкіна Ірина Валеріївна _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2024

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти — другий (магістерський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2024 р.

ЗАВДАННЯ
на магістерську дисертацію

Студент: Бондаренко Андрій Андрійович

1. Тема роботи: «*Аналіз стійкості протоколів консенсусу Proof-of-history і Proof-of-authority до атак централізації та їх застосування в задачі оцінки якості IOC*», науковий керівник дисертації: професор, д.т.н., с.н.с. Кудін Антон Михайлович,

затверджені наказом по університету №__ від «__» _____ 2024 р.

2. Термін подання студентом роботи: «__» _____ 2024 р.

3. Об'єкт дослідження: процес виявлення вторгнень системами IDS побудованих за децентралізованим принципом (на основі блокчейну).

4. Предмет дослідження: стійкість PoS протоколів PoH та PoA, що використовуються в цих децентралізованих систем виявлення вторгнень та оцінка якості індикаторів компрометації в цих системах виявлення вторгнення.

5. Перелік завдань:

– провести огляд опублікованих джерел за тематикою дослідження;

– проаналізувати існуючі методи кількісної оцінки якості IOC, враховуючи фактору зміни кількісної оцінки якості IOC з плином часу;

– застосувати в якості кількісної оцінки якості IOC блокчейн технологій на протоколах Proof-of-History та Proof-of-Authority;

– оцінити стійкість Proof-of-History та Proof-of-Authority від відомих атак.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: Презентація доповіді.

7. Орієнтовний перелік публікацій: XXII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «ТЕОРЕТИЧНІ І ПРИКЛАДНІ ПРОБЛЕМИ ФІЗИКИ, МАТЕМАТИКИ ТА ІНФОРМАТИКИ» (13 - 17 травня 2024 р., м. Київ, Україна).

8. Дата видачі завдання: 10 вересня 2023 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2023 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2023 р.	Виконано
3	Вибір напрямку досліджень та конкретизація задач	Листопад-січень 2023 р.	Виконано
4	Аналізувати існуючі методи кількісної оцінки якості IOC, враховуючи фактору зміни кількісної оцінки якості IOC з плином часу	Лютий-березень 2024 р.	Виконано
5	Оцінка стійкості Proof-of-History та Proof-of-Authority від відомих атак	Квітень-травень 2024 р.	Виконано
6	Оформлення дипломної роботи	Червень 2024 р.	Виконано

Студент _____ Андрій БОНДАРЕНКО

Керівник _____ Антон КУДІН

РЕФЕРАТ

Кваліфікаційна робота містить: 51 стор., 3 рисунки, 6 джерел.

Метою дослідження є оцінка стійкості протоколів Proof-of-history та Proof-of-authority від відомих атак на протоколи PoS типу для кількісної оцінки якості IOC.

Об'єктом дослідження є процес виявлення вторгнень системами IDS побудованих за децентралізованим принципом (на основі блокчейну).

Предметом дослідження є стійкість PoS протоколів PoH та PoA, що використовуються в цих децентралізованих систем виявлення вторгнень та оцінка якості індикаторів компрометації в цих системах виявлення вторгнення.

У цій роботі досліджено стійкість протоколів консенсусу Proof-of-history та Proof-of-authority до відомих атак на протоколи Proof-of-Stake (PoS) типу для кількісної оцінки якості IOC, яка змінюється з плином часу. Ця кількісна міра змінюється за допомогою блокчейну.

ІНДИКАТОРИ КОМПРОМЕТАЦІЇ, БЛОКЧЕЙН, PROOF-OF-STAKE, PROOF-OF-HISTORY, PROOF-OF-AUTHORITY

ABSTRACT

The thesis has 51 pages, 3 figures, 6 sources.

The study aims to estimate the security of the Proof-of-history and Proof-of-authority protocols against known attacks on PoS-type protocols.

The study's object is the intrusion detection process by IDS systems built on a decentralised principle (based on the blockchain).

The subject of this research is the security of the PoH and PoA protocols used in these decentralised intrusion detection systems and the quality assessment of compromise indicators in these intrusion detection systems.

In this paper, we investigate the security of the Proof-of-history and Proof-of-authority consensus protocols against known attacks on Proof-of-Stake (PoS) type protocols to quantify the time-varying quality of IOCs. This quantitative measure is changed using the blockchain.

INDICATORS OF COMPROMISE, BLOCKCHAIN, PROOF-OF-STAKE, PROOF-OF-HISTORY, PROOF-OF-AUTHORITY

ЗМІСТ

ВСТУП

Актуальність дослідження. Актуальність даного дослідження визначається невирішеністю проблеми побудови систем виявлення вторгнень з кількісними оцінками ефективності їх роботи.

Метою дослідження є оцінка стійкості протоколів Proof-of-history та Proof-of-authority від відомих атак на протоколи PoS типу для кількісної оцінки якості IOC. Для досягнення мети необхідно розв'язати **задачу дослідження**, яка полягає в:

1) аналізі існуючих методів кількісної оцінки якості IOC;

2) врахування фактору зміни кількісної оцінки якості IOC з плином часу;

3) застосування в якості кількісної оцінки якості IOC блокчейн технологій на протоколах Proof-of-History та Proof-of-Authority;

4) оцінка стійкості Proof-of-History та Proof-of-Authority від відомих атак.

Для розв'язання задачі необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) проаналізувати існуючі методи кількісної оцінки якості IOC, враховуючи фактору зміни кількісної оцінки якості IOC з плином часу;

3) застосувати в якості кількісної оцінки якості IOC блокчейн технологій на протоколах Proof-of-History та Proof-of-Authority;

4) оцінити стійкість Proof-of-History та Proof-of-Authority від відомих атак.

Об'єктом дослідження є процес виявлення вторгнень системами IDS побудованих за децентралізованим принципом (на основі блокчейну).

Предметом дослідження є стійкість PoS протоколів PoH та PoA, що використовуються в цих децентралізованих систем виявлення вторгнень та оцінка якості індикаторів компрометації в цих системах виявлення вторгнення.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: теорія імовірностей, комбінаторний аналіз.

Наукова новизна отриманих результатів полягає тому, що вперше досліджені атаки на протоколи PoA, які використовуються, які використовуються в децентралізованих системах виявлення вторгнень.

Практичне значення результатів полягає в можливості побудови нових IDS.

Апробація результатів та публікації. Частину результатів, одержаних в ході виконання дослідження було представлено на XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «ТЕОРЕТИЧНІ І ПРИКЛАДНІ ПРОБЛЕМИ ФІЗИКИ, МАТЕМАТИКИ ТА ІНФОРМАТИКИ» (13 - 17 травня 2024 р., м. Київ, Україна).

1 ІСНУЮЧІ МЕТОДИ КІЛЬКІСНОЇ ОЦІНКИ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ ТА МОЖЛИВІСТЬ ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ВИРІШЕННЯ ЦИХ ЗАДАЧ

1.1 Індикатори компрометації

У сучасному світі, де бізнес значною мірою покладається на цифрову інфраструктуру, захист конфіденційної інформації має першочергове значення для стійкості організації. В умовах постійного тиску кіберзагроз проактивне виявлення та пом'якшення наслідків потенційних атак стало запорукою ефективних систем кібербезпеки. Зловмисники безперервно намагаються використати вразливості в людях, процесах або технологіях. Тому організації використовують способи запобігання потенційним збиткам або виявлення і реагування на загрози в режимі онлайн, щоб локалізувати інциденти і відновити роботу.

Використання IOC має важливе значення для ефективного виявлення загроз і реагування на них. IOC слугують основою безпекових операцій, що ґрунтуються на розвідці загроз, дозволяючи організаціям передбачати і запобігати кібератакам до того, як вони завдадуть значної шкоди. Інтегрувавши IOC у свою систему кібербезпеки та використовуючи передові можливості аналітики та машинного навчання, організації можуть випереджати постійно мінливий ландшафт загроз, захищаючи свої цифрові активи і зберігаючи безперервність операційної діяльності.

Індикатори компрометації (англ. indicators of compromise, IOC) - це цифрові артефакти, такі як IP-адреси, домени, URL-адреси, геші файлів, ключі реєстру, шаблони мережевого трафіку, які отримуються в результаті експертиз, розвідки загроз, реверс-інжинірингу тощо, і служать доказами та допомагають встановити відповідальних за

кібератаки. Іншими словами, IOC - це будь-яка інформація, яку ми можемо використати для виявлення атаки. Сюди входять різні артефакти або підписи, які можуть допомогти у розпізнаванні атаки, що уможливить її подальшу ідентифікацію. Життєвий цикл IOC проходить через певні етапи: створення/збір/отримання переліку індикаторів компрометації, використання інструментів моніторингу та інших засобів виявлення для виявлення підозрілих дій, збирання інформації щодо наявних в середовищі IOC, проведення аналізу для вивчення та навчання з цих IOC, та списання IOC.

DDoS - це навмисна спроба порушити нормальний трафік цільового сервера, сервісу чи мережі, перевантажуючи ціль або її інфраструктуру потоком інтернет-трафіку. Звичайно, що найбільш очевидною ознакою DDoS атаки є уповільнення або недоступність сайту чи сервісу, але низка чинників, таких як звичайне збільшення трафіку, можуть призводити до схожих проблем з продуктивністю, зазвичай потрібне подальше розслідування. Коли справа доходить до виявлення потенційних DDoS атак, інструменти аналізу трафіку можуть допомогти виявити кілька ознак, які можуть вказувати на поточну або майбутню DDoS-атаку. Одним з таких індикаторів є підозрілий обсяг трафіку, що надходить з однієї IP адреси або з діапазону IP-адрес, що саме по собі може бути IOC. Іншим індикаторм є великий трафік від користувачів, які мають однаковий поведінковий профіль, наприклад, однаковий тип пристрою, геолокацію або версію веб-браузера, що може свідчити про наявність ботнету. Крім того, незрозумілий сплеск запитів до однієї сторінки або кінцевої точки на вашому веб-сайті або додатку може бути ознакою DDoS атаки, яка намагається перевантажити ваші ресурси. Про зловмисну активність також можуть свідчити дивні патерни трафіку, такі як сплески в незвичні години доби або патерни, які виглядають неприродно, наприклад, сплеск, що відбувається кожні 10 хвилин.

Іншою поширеною атакою є атака шкідливого коду. Ця атака може завдати серйозної шкоди, вивести з ладу системи, викрасти конфіденційні

дані або надати зловмиснику несанкціонований доступ. Існує низка індикаторів, на які слід звертати увагу, щоб виявити цей вид зловмисної активності.

Один з них - це перевірка гешів файлів за базою даних відомих шкідливих файлів, корисних навантажень, скриптів тощо. Наявність збігів є гарною ознакою того, що відбувається щось підозріле. Ми також відстежуємо з'єднання ураженої системи з тіньовими IP-адресами, пов'язаними з C2 або іншою шкідливою інфраструктурою. Так само шкідливе програмне забезпечення часто спілкується через домени, які позначені як хостинг або розповсюдження шкідливого коду.

На самому хості ми шукаємо дивні ключі реєстру, які модифікуються, нерегулярні шаблони мережевого трафіку, файли, які записуються в несподівані місця, або процеси, які демонструють показову поведінку, наприклад, впровадження коду або підробку пам'яті. Іноді шкідливе програмне забезпечення використовує mutex об'єкти, щоб уникнути запуску декількох екземплярів - побачити одне з таких унікальних імен mutex може підказати нам, що до чого. Те саме стосується виявлення незнайомих служб, процесів або недійсних/відкликаних цифрових підписів, пов'язаних з відомими загрозами. Загалом, ми аналізуємо цілу низку показників, щоб визначити, чи була система скомпрометована шкідливим кодом.

Ще однією поширеною атакою є отримання доступу до систем, до яких не мав би. Потрібно бути напоготові і стежити за будь-якими ознаками цього. Існує безліч індикаторів, які можуть свідчити про те, що зловмисник отримав несанкціонований доступ. Багато невдалих спроб входу з різних IP-адрес - класична ознака того, що хтось намагається зламати систему або використовує викрадені облікові дані. Або якщо ви бачите, що облікові записи користувачів поводяться дивно - входять в систему в дивний час, з незнайомих місць, роблять те, що зазвичай не роблять, - це може бути скомпрометований обліковий запис.

Також слід звертати увагу на випадки підвищення привілеїв, такі

як створення нових облікових записів адміністратора, розширення прав користувачів або втручання в основні файли та налаштування. Запуск нових, невідомих процесів або несанкціонований мережевий трафік є настільки ж непередбачуваним. Дірки в журналах аудиту, випадкові пристрої, підключені до мережі, встановлені бекдори - все це тривожні сигнали. Навіть такі дрібниці, як зміна конфіденційних файлів, коли вони не повинні бути змінені, можуть натякати на злом. І, звичайно, якщо ви виявляєте будь-які дані, що залишають мережу без дозволу, це величезний червоний прапор, який вказує на те, що витік даних йде на спад. Правило гри полягає в тому, щоб залишатися холоднокровними і ловити ці індикатори компрометації до того, як вони перетворяться на повномасштабний кошмар безпеки.

Параметри інцидентів

Невід'ємною частиною реагування на інциденти є аналіз, який може дати IOC, характерні для конкретної атаки або кампанії. Для отримання IOC необхідно зібрати та ретельно проаналізувати дані про інцидент. І навпаки, Індикатори компрометації слід співвідносити з конкретним інцидентом. У контексті кібербезпеки інцидент включає кілька ключових параметрів, такі як зловмисник (суб'єкт відповідальний за атаки), ціль (як ваша система була взламана), час (коли ваша система була взламана), тяжкість (серйозність інциденту), реагування (на чому потрібно зосередити зусилля з реагування або пом'якшення наслідків) та довіра (чи був певний IOC правильним для інциденту).

З часом довіра до IOC буде знижуватися. Це вимагає складної оцінки параметрів для вимірювання залежної від часу достовірності IOC. Важливими для такого розуміння є параметри IOC, які змінюються з часом. До них відносяться джерело, що позначає IDS, honeypot або інші системи, які виявили IOC. Мітка часу позначає дату і час початкового звіту про IOC. Пов'язані імпульси - це сигнали про виникнення IOC з

різних каналів, кожному з яких присвоєно рівень довіри відносно джерела. Мітка часу імпульсу фіксує дату і час звіту про імпульс. MISP пропонує широку класифікацію параметрів, яка є корисною для нашої роботи. Ці параметри можуть бути використані для відстеження часового спаду актуальності IOC. Зокрема, в системі AlienVault серед безлічі параметрів важливе значення мають пов'язані з ними сповіщення, імпульси (які слугують для перевірки IOC і його виявлення альтернативним джерелом) і джерело IOC. При спільному використанні ці параметри дають повне і динамічне розуміння ситуації із загрозами кібербезпеці.

Оцінка IOC

В умовах розвитку кібербезпеки зростає кількість вдосконалених IOC. Однак попередні зловмисні кампанії та методи залишаються активними. Рішення для боротьби з порушеннями включає в себе не тільки розробку більш унікальних передових індикаторів, а й підтримку якості, цінності та довіри до існуючих індикаторів. Вивчення недоліків і обмежень попередніх моделей та індикаторів має вирішальне значення.

Для підвищення довіри до IOC необхідно оцінювати їх, що також збільшує термін їх служби. Наразі не існує узагальненого методу оцінки довіри до IOC. Довіру можна пояснити як оцінку, яка відображає надійність конкретного IOC з плином часу.

Для оцінювання індикаторів запропонована модель оцінки, яка може бути застосована до кожного типу індикатора або джерела даних. Ця модель складається з початкового значення та коефіцієнта спаду. Початкове значення життєвого циклу індикатора або оцінка індикатора, що перезавантажується при введенні нового індикатора та зважуванні достовірності його джерела, таксономії, що також додається до нього, називається базовою оцінкою. Коефіцієнт спаду визначає швидкість, з якою оцінка зменшується з плином часу.

Цінність IOC оцінюється на основі цього показника. При оцінці IOC розраховується коефіцієнт спаду, а також інші фактори. Важливо регулярно оцінювати показники на всіх доступних платформах даних.

Окрім оцінювання, потрібна певна метрика для визначення індикаторів та джерел даних, що дозволить визначити їхню достовірність. Сьогодні існує багато джерел IOC та платформ. Однак їхня якість і достовірність викликають сумніви через хибні спрацьовування.

Спад індикаторів

Точність і надійність інформації в кібербезпеці є надзвичайно важливими. Однак хибні спрацювання все ще можуть траплятися. Для захисту атрибутів застосовуються різні заходи безпеки, такі як блокування дій на основі типу спільного атрибуту (наприклад, IP-адреси або гешу). Коли організації прагнуть пов'язати та співвіднести атрибути з додатковими загрозами, їм потрібні точні та надійні дані.

Для зменшення значущості атрибутів використовується метод підрахунку балів, який використовує класифікацію та надійність джерел. Кожен атрибут має унікальну швидкість занепаду, яка змінюється залежно від типу атрибуту. Наприклад, швидкість занепаду початкового індикатора є низькою, але з плином часу активність індикаторів загроз може зростати або зберігатися. Блокуючи або запобігаючи цим загрозам, організації можуть посилити свою безпеку.

Не існує заздалегідь визначеного максимального терміну служби для конкретного IOC. Однак серед фахівців з безпеки існує загальне розуміння того, що різні типи IOC не можуть мати однаковий термін служби. Наприклад, IP-адреси зазвичай мають термін дії від кількох днів до кількох тижнів, оскільки вони часто повторно використовуються різними користувачами або стають застарілими зі зміною конфігурації мережі. Для доменних імен тривалість життя може бути різною, але зазвичай становить від кількох тижнів до кількох місяців. Доменні імена

можуть втратити чинність і перейти до нових власників або застаріти, оскільки організації змінюють свою присутність в Інтернеті. Тривалість життя URL-адрес подібна до тривалості життя доменних імен і становить від кількох місяців до кількох років. Для деяких конкретних шкідливих кампаній URL-адреси можуть занепадати від кількох днів до кількох тижнів. Тривалість життя гешу файлів зазвичай довша, ніж у IP-адрес або доменних імен, і становить від кількох місяців до кількох років. Однак можуть траплятися помилкові спрацьовування, тому організаціям може знадобитися періодично переглядати та оновлювати свої дані про загрози. Для адрес електронної пошти тривалість життя зазвичай становить від кількох днів до кількох років, оскільки адреси електронної пошти можна легко створювати та видаляти.

Важливо розуміти, що ці терміни життя є лише приблизними і можуть коливатися залежно від конкретного IOC та контексту його використання. Крім того, тривалість життя деяких IOC може бути коротшою або довшою, залежно від рівня загрози, яку вони становлять, або ступеня уваги, яку вони привертають з боку зловмисників.

1.2 Proof-of-Work

Proof-of-Work (PoW) - це протокол консенсусу, заснований на доведенні виконаної роботи. У цій моделі консенсусу вузли, що діють як майнери, намагаються вирішити обчислювальну задачу. Вузол, який першим розв'язує задачу, підтверджує і додає новий блок транзакцій до блокчейну. Виконані дії винагороджуються для першого успішного майнера, що заохочує конкуренцію. Завдання розроблено таким чином, щоб його було важко вирішити, але легко перевірити отримане рішення. Це дозволяє всім іншим вузлам мережі легко перевіряти будь-які запропоновані наступні блоки, і будь-який блок, який не відповідає умовам задачі, буде відхилений. Однак генерація блоків вимагає залучення великих обчислювальних потужностей і вносить затримку для

підтвердження блоків, що призводить до низької ефективності і низької пропускної здатності транзакцій. Тому PoW погано адаптується до реальних сценаріїв, в яких існує висока швидкість транзакцій і попит на масштабованість мережі.

Поширеною технікою є вимога, щоб геш-значення заголовка блоку було меншим за певне цільове значення. Ноди намагаються знайти таке значення для nonce (одного з атрибутів блоку), щоб геш всього блоку (список транзакцій, геш попереднього блоку і саме значення nonce) отримав необхідне значення (визначається кількістю початкових нулів; тобто результат повинен потрапляти в невелику область в порівнянні з усім вихідним простором). Єдиний спосіб досягти успіху у вирішенні цієї геш-головоломки, якщо геш-функція є криптографічною, - це просто перебирати значення nonce до тих пір, поки результат не потрапить в потрібну область. Зокрема, якщо набір можливих значень становить лише 1% від загального простору, то для досягнення успіху потрібно буде перебрати в середньому близько 100 значень.

Вузли вносять багато невеликих змін в nonce в заголовку свого блоку, намагаючись знайти геш-значення, яке має відповідну кількість початкових нулів. Для кожної такої спроби вузол повинен обчислити геш для всього заголовка блоку. Багаторазове гешування заголовка блоку стає обчислювально інтенсивним процесом, що забирає багато часу.

Цільове значення може бути скориговане з часом, щоб налаштувати складність і вплинути на частоту публікації блоків. Спочатку геш-значення, як правило, має містити певну кількість початкових нулів, що впливає на інтенсивність видачі блоків. Збільшення кількості початкових нулів збільшує складність завдання, оскільки таких геш-значень стає менше і їх важче знайти. Зменшення кількості початкових нулів знижує рівень складності, оскільки збільшується кількість можливих геш-значень.

Таке коригування необхідне для підтримки обчислювальної складності завдання і, таким чином, для підтримки основного механізму

безпеки конкретної криптовалютної мережі. Доступна обчислювальна потужність з часом збільшується, як і кількість вузлів, тому складність завдання зазвичай зростає.

Регулювання цільового значення має на меті запобігти тому, щоб жоден користувач не зміг перебрати на себе виробництво блоків, тобто не допустити централізації. Тому криптовалюти з доказом роботи вимагають, щоб кожен користувач, який створив блок, довів, що в його створення було вкладено значний обсяг роботи, щоб ненадійні учасники, які хочуть модифікувати попередні блоки, працювали важче, ніж чесні колеги.

Порядок генерації блоків кожним учасником непередбачуваний, оскільки все залежить від обчислювальних можливостей користувачів. Часто ця робота виконується не безкоштовно - вузли намагаються вирішити цю складну задачу, щоб отримати певну винагороду (зазвичай у вигляді криптовалюти, яку пропонує мережа блокчейн). Винагорода, отримана за розширення і підтримку блокчейну, називається системою винагороди або моделлю стимулювання.

Після виконання цієї роботи вузол надсилає свій блок з дійсним одноразовим записом усім вузлам мережі блокчейн. Інші вузли отримують, перевіряють, чи відповідає новий блок вимогам завдання, і додають його до своєї копії блокчейну. Таким чином, новий блок швидко поширюється мережею вузлів-учасників.

1.3 Proof-of-Stake

Proof-of-Stake - це протокол консенсусу, який залежить від того, скільки коштів у вигляді криптовалюти інвестував кожен користувач в систему. Мережа довіряє лише тим користувачам, що володіють значною сумою коштів у вигляді криптовалюти. Внесок криптовалюти в блокчейн-систему є тим фактором, що дозволяє визначати, який користувач буде генерувати наступний блок. Чим більша частка у

загальній сумі мережі, тим є більші шанси на генерацію наступного блоку. Імовірність отримати винагороду тепер чітко залежатиме від того, який користувач вклав більше інвестицій. Така модель не потребує виконання доведення роботи і дозволяє заощадити багато енергоресурсів та часу. Принцип роботи протоколу можна привести на прикладі банку, в який всі учасники мережі закладають свої криптоактиви, і потім очікують на випадкове обрання для генерації блоку, що здійснюється на основі голосування, яке залежить від частки депозиту в загальній сумі вкладу. Процедура обрання майнеру є ймовірнісною. Але перевага при виборі, зазвичай, стоїть за багатшими, тому вони більше отримують вигоди від такого протоколу консенсусу, що вказує на деяку централізацію. Далі особа, що створює інвестицію, матиме назву стейкхолдер, а розмір інвестиції будемо називати стейк. Відповідно імовірність того, що стейкхолдер буде генерувати наступний блок, буде пропорційною долі його стейку серед всіх користувачів. Існують процедури голосування такі, що не дозволяють вплинути стейкхолдеру на генерацію наступних блоків. Також визначимо, що на деякому проміжку часу можна згенерувати багато блоків, цей інтервал називають епохою. Епоха розбивається на таймслоти - проміжки часу, де протягом кожного такого інтервалу можна згенерувати лише один блок. Якщо кількість таймслотів в одній епосі менша, ніж кількість стейкхолдерів, тоді хтось може не потрапити в епоху, потрапити у наступну. У кого великий стейк, той має можливість генерувати кілька блоків протягом однієї епохи. У такій системі Proof-of-Work існує, але він націлений на створення нових монет. В кожну епоху стейкхолдери потрапляють ймовірнісно. Коли учасники вносять внески, то ці внески блокуються в системі на кілька епох вперед. Якщо деякий учасник захоче забрати свої кошти, він про це оголошує та чекає кілька епох. Дана процедура створена з метою підтримки безпеки мережі, у випадку, коли в системі спостерігається певна централізація щодо користувача, що має великий внесок криптоактивів у мережі, і до нього може виникнути підозра в намаганні виконати нечесні дії, що призведе до

деваляції коштів всієї мережі. Іноді генерація наступного блоку у розглянутих протоколів консенсусу відбувається одночасно у двох користувачів, і система має два ланцюги, які виходять з деякого попереднього блоку, таке явище називається форком, і воно зустрічається лише в випадках незлагодженої несинхронізованої роботи мережі, або при спробі компрометувати мережу виконуючи атаки. В таких випадках працює правило найдовшого ланцюга: гілка вважається валідною, якщо вона є найдовшою (насправді кількість енергії вкладеної в неї є більшою), оскільки на її створення було витрачено більше ресурсів та часу, і майнери більше зацікавлені в таких ланцюгах через винагороду, яку вони отримують унаслідок створення блоку.

Стейк (вклад)-особисті кошти у певній криптовалюті, які поклали на депозит і заморозили. Нехай $P1$,...,Pn-стейкхолдери, α_1,...,α_n-стейки стейкхолдерів,$\alpha_=\alpha_1 + ... + \alpha_n$-спільний стейк. Кожну епоху має N блоків, де кожен блок повинен бути згенерований протягом відповідного часового інтервалу (timeslot TS), відповідним слот лідером. Слот лідера обираємо використовуючи Verifyable Random Function (VRE) для наступної епохи, де для кожного інтервалу ймовірність того, що P стане слот лідером пропойціна $\frac{\alpha_i}{\alpha}$

1.4 Proof-of-Authority

Proof-of-Authority (PoA) - це протокол консенсусу, відомий своєю ефективністю та швидкістю перевірки транзакцій в мережах блокчейн. Однією з його основних переваг є енергоефективність, що робить його більш стійким варіантом у порівнянні з енергоємними алгоритмами консенсусу, такими як Proof-of-Work. Крім того, мережі PoA працюють швидко, забезпечуючи швидку обробку транзакцій і перевірку блоків. Однак, важливо відзначити, що PoA має свої недоліки. Одним з істотних недоліків є його тенденція до централізації. Хоча PoA технічно може використовуватися в публічних блокчейнах, він частіше застосовується в

приватних блокчейнах, де обрана група затверджених валідаторів контролює процес валідації. Така централізована природа може викликати занепокоєння щодо децентралізації та стійкості мережі до цензури, що суперечить ідеалам багатьох ентузіастів блокчейну.

У мережах на основі PoA транзакції і блоки проходять перевірку авторизованими акаунтами, так званими валідаторами, які виконують програмне забезпечення для організації транзакцій у блоки. Ця процедура працює автоматично, звільняючи валідаторів від необхідності постійно контролювати свої комп'ютерні системи. Тим не менш, вона вимагає підтримки комп'ютера, призначеного в якості вузла повноважень, в безпеці і безкомпромісності.

Для створення валідатора необхідно виконати три основні умови:

1) ідентичність повинна бути формально перевірена в ланцюжку, з можливістю перехресної перевірки інформації в загальнодоступному домені

2) отримати право на валідацію блоків має бути складно, щоб право на валідацію блоків було зароблением і цінним. (Приклад: потенційні валідатори повинні отримати ліцензію державного нотаріуса)

3) Повинна бути повна одноманітність у перевірках і процедурах встановлення повноважень.

PoA надає особам привілей служити валідаторами, стимулюючи їх підтримувати досягнуту позицію. Пов'язуючи репутацію з особистістю, валідатори мотивовані підтримувати цілісність процесу транзакцій, оскільки вони не бажають заплямувати свою особистість негативною репутацією, що може поставити під загрозу їхній важко зароблений статус валідатора.

1.5 Proof-of-History

Фундаментальна концепція полягає в тому, що довіра має зміщуватися від простого покладання на часову позначку транзакції.

Натомість метою є встановлення достовірних доказів того, що транзакція відбулася до або після певної події.

Розглянемо сценарій фотографування на фоні останнього випуску New York Times. Ця дія слугує матеріальним доказом того, що фотографія була зроблена після публікації газети. По суті, це все одно, що сказати: «Дивіться, у мене є ця фотографія, зроблена на тлі сьогоднішньої газети, отже, вона повинна була бути зроблена сьогодні, якщо тільки я не контролюю те, що друкує газета». Аналогічно, Proof-of-History працює за цим принципом, дозволяючи створити хронологічний запис, який беззаперечно підтверджує, що подія відбулася в певний момент часу.

Тепер давайте заглибимося в технічний аспект. Механізм Proof-of-History функціонує як високочастотна функція затримки з можливістю перевірки (Verifiable Delay Function, VDF). VDF вимагає заздалегідь визначеної послідовності кроків для оцінки, що дає чіткий результат, який може бути легко і ефективно перевірений громадськістю.

Ця конкретна реалізація використовує послідовну геш-функцію, стійку до атак на попередні зображення, яка постійно повторюється, при цьому попередній результат слугує наступним входом.Через певні проміжки часу в журнал записується як кількість, так і поточний результат. Примітно, що при використанні геш-функції SHA256 цей процес неможливо розпаралелити, не вдаючись до методу грубої сили із залученням астрономічної кількості обчислювальних ядер (2^{128} ядер, якщо бути точним).

Важливість полягає в тому, що можна бути впевненим, що між кожним поколінням лічильників пройшли реальні часові інтервали, а порядок запису кожного лічильника точно відображає його хронологічну появу. Це не тільки зміцнює цілісність записаних даних, але й підвищує загальний рівень безпеки, створюючи надійну основу для перевірки часових послідовностей у транзакціях.

Як написано у [5]: «У нерозділеному стані в будь-який момент часу

в мережі є один Лідер. Кожен вузол Верифікатора має ті ж самі апаратні можливості, що і Лідер, і може бути обраний Лідером, це робиться за допомогою виборів на основі PoS.»

Вибори нового генератора PoH відбуваються, коли виявлено несправність генератора PoH. Валідатор з найбільшою кількістю голосів, або з найбільшою адресою відкритого ключа, якщо вони розділилися порівну, обирається новим генератором PoH. Для нової послідовності потрібна переважна більшість підтверджень. Якщо новий лідер зазнає невдачі до того, як буде отримано переважну більшість підтверджень, обирається наступний за рейтингом валідатор, і потрібен новий набір підтверджень. Щоб поміняти голоси, валідатор повинен проголосувати на лічильнику послідовності з вищим значенням PoH, і новий голос повинен містити голоси, які він хоче поміняти. В іншому випадку другий голос буде викреслено. Перемикання голосів має бути спроектовано таким чином, щоб воно могло відбуватися лише на висоті, яка не має супербільшості. Після створення генератора PoH може бути обраний вторинний генератор, який візьме на себе обов'язки з обробки транзакцій. Якщо вторинний генератор існує, він буде вважатися наступним лідером під час збою первинного. Платформа розроблена таким чином, що вторинний генератор стає первинним, а генератори нижчого рангу підвищуються в разі виявлення винятків або за заздалегідь визначеним розкладом.

$H(t+1) = VDF(H(t||data))$, де $H(t)$ - значення гешу в момент часу t, $H(t+1)$ - значення гешу на наступному часовому кроці $t+1$, $VDF()$ - функція затримки, що перевіряється, $data$ - данні, які можуть бути порожньою.

Висновки до розділу 1

У цьому розділі розглянуто індикатори компрометації та їхню роль у виявленні та реагуванні на кіберзагрози. Обговорено різні типи

кібератак, такі як DDoS-атаки та атаки шкідливого ПЗ, та відповідні їм IOC. Розглянуто методи оцінки IOC та важливість точних даних. Також розглянуто протоколи консенсусу Proof-of-Work, Proof-of-Stake, Proof-of-Authority та Proof-of-History. Розуміння яких має вирішальне значення для розуміння того, як працюють різні мережі блокчейн і як вони досягають консенсусу.

2 МОДЕЛЬ ТА МЕТОДИКА КІЛЬКІСНОЇ ОЦІНКИ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ З ЗАСТОСУВАННЯМ БЛОКЧЕЙН-ТЕХНОЛОГІЙ, ЩО ВРАХОВУЄ ВПЛИВ ЧАСУ

2.1 Модель оцінки IOC

У сфері кібербезпеки рівень довіри важливий для визначення достовірності IOC. Він допомагає зменшити помилкові позитивні результати та віддати перевагу завданням, пов'язаним з новими загрозами. Рівень довіри вимірюється на шкалі від 0 до 1 та розраховується на основі надійності джерела. У цьому дослідженні рівень довіри для IOC розраховується для двох різних потоків, обом потокам присвоєно значення довіри 0,5. Значення довіри відіграє значну роль у визначенні рівня довіри, який, в свою чергу, впливає на зниження індикаторів.

У цій статті [4] представлено модель оцінки, яка інтегрує відкриті канали розвідки загроз з метою створення більш ефективної системи оцінювання для IOC, яка покликана знизити рівень помилкових спрацьовувань. Механізм оцінки моделі залежить від часу, включаючи функцію часу розпаду, отриману з попередніх досліджень. Достовірність розвідувальної інформації визначається шляхом розрахунку довіри до джерела, яка враховує такі фактори, як обсяг інформації, її оперативність, повнота і ступінь збігу з білим списком. Дуже важливо оцінювати кожен IOC, оскільки нові імпульси (випадки IOC) з'являються при надходженні з різних джерел. Однак рівень довіри ніколи не повинен перевищувати максимальний поріг 1, який означає повну довіру і означає, що ми приймаємо всі імпульси від джерела без жодних застережень. Для спрощення та збереження універсальності моделі, значення довіри 0.5 присвоюється будь-якому джерелу, достовірність якого не була

встановлена.

Модель була розроблена для розрахунку довірчої оцінки (*trust* value) IOC протягом усього життєвого циклу. Для підрахунку $pulse_i$ (значення імпульсу для певного i-го IOC) була запропонована формула:

$$pulse_i = logistic(\sum_{j=1}^{N} trust_{ij}) \tag{2.1}$$

де $trust_{ij}$ - рівень довіри до j-го джерела імпульсів в діапазоні $(0 \dots 1)$; N - кількість цих джерел; $score_i$ - поточна оцінка довіри для i-го IOC; нарешті, $logistic(.)$ - функція нормалізації, яка приводить суму довіри декількох джерел до діапазону $(0 \dots 1)$. І оскільки оцінка довіри також належить до того ж діапазону, значення імпульсу також нормалізується до $(0 \dots 1)$.

Запропоновану модель було протестовано з урахуванням значення довіри на різних часових проміжках для відстеження змін у поведінці рівня довіри. Ця вдосконалена версія дозволяє відображати очікуваний рівень довіри в різних часових масштабах, таких як дні та години.

Значення часу не можна недооцінювати, оскільки він безпосередньо впливає на спад індикатора або пов'язаних з ним довірчих інтервалів. Для тих інтервалів, де виявлено імпульси, метод визначення довірчої ймовірності полягає в наступному:

$$c_t = logistic(c_t^{decayed} + pulse_i) \tag{2.2}$$

де $c_t^{decayed}$ визначено як:

$$c_t^{decayed} = \frac{c_{t-1} - k * c_{t-1}(m - c_{t-1})}{m^2}, \tag{2.3}$$

$$f = \frac{a}{1 + \exp^{-k \cdot (b \cdot x - x_0)}}, \tag{2.4}$$

де c_t – рівень довіри в момент часу t; k – константа для регулювання швидкості спаду довіри відповідно до максимального терміну служби IOC; i – діапазон випадків/періодів. Варто зазначити, що рівняння (2.3) є

скінченно-різницевою формою оберненої логістичної функції (рівняння (2.4) з $k < 0$ та $a = m$). У період відсутності імпульсних сигналів обчислення значення c_t визначається виключно за рівнянням (2.3).

Для вирішення проблеми різної якості джерел IOC ми пропонуємо децентралізований підхід з використанням технології блокчейн і протоколу консенсусу PoRep [3]. Система включає динамічний рейтинг IOC, який кількісно оцінює надійність кожного учасника, що надає IOC в мережу. Важливо, що рейтинг IOC користувача з часом поступово знижується, якщо не спостерігається подальшої зловмисної активності, імітуючи природний занепад застарілих показників.

Рейтинг IOC, що зменшується з часом, інтегрований у консенсусний протокол PoRep, де учасники з вищою репутацією, що випливає з постійного надання високоякісних та оновлених даних IOC, отримують пропорційно більший вплив на перевірку та додавання нових даних IOC до децентралізованого реєстру. Це стимулює безперервне надання якісних розвідувальних даних про загрози і водночас поступово виключає неактивних або скомпрометованих учасників, чия репутація погіршується. Прозорий, саморегульований характер запропонованої системи сприяє створенню стійкої, надійної екосистеми, яка забезпечує цілісність і надійність колективно використовуваних IOC, зменшуючи ризики, пов'язані з розповсюдженням неточної або застарілої інформації.

Крім того, PoRep [2] не припускає, що майнери завжди заслуговують на довіру, тому вимагає моніторингу дій майнерів і виключення зловмисних вузлів з мережі. PoRep пропонує механізми моніторингу та голосування, які мають на меті бути більш ефективними, ніж попередні механізми візантійської відмовостійкості (BFT). У PoRep найстаріші вузли мережі обираються для майнінгу відповідно до критерію зрілості. Майнери по черзі видобувають кожен новий блок по колу. За кожним майнером стежить випадково вибране журі, яке оцінює репутацію майнерів відповідно до порогу довіри, необхідного для мережі.

Якщо репутація майнера нижча за поріг довіри, журі голосує за виключення цього майнера. Крім того, механізм контролю доступу самоорганізовує мережу, змінюючи необхідну кількість майнерів для підтримки масштабованості мережі.

2.2 CVE та MITRE ATT&CK

Common Vulnerabilities and Exposures (CVE) створена некомерційною організацією MITRE у 1999 році, CVE являє собою каталог із стислими описами вразливостей, які включають інформацію про вразливі версії програм, виробників, типи вразливостей та унікальні ідентифікаційні номери для кожної виявленої вразливості. Ця класифікація стала стандартом в індустрії кібербезпеки та широко використовується фахівцями для відстеження та усунення потенційних загроз.

Хоча CVE, строго кажучи, є класифікацією вразливостей, а не кібератак, її можна розглядати як корисний ресурс для розуміння способів, якими зловмисники можуть атакувати програмне забезпечення. Опис кожної вразливості у CVE дає уявлення про те, як певна програма може бути скомпрометована, що дозволяє фахівцям з кібербезпеки розробляти ефективні контрзаходи та стратегії захисту. Таким чином, CVE не лише каталогізує вразливості, але й є цінним джерелом інформації про потенційні векторы атак.

Одними з головних переваг CVE є її широка популярність серед фахівців з кібербезпеки та швидкість оновлення. Оскільки ця база даних є загальновизнаним стандартом, вона забезпечує спільну мову для опису вразливостей, що полегшує співпрацю та обмін інформацією між організаціями та експертами. Крім того, CVE регулярно оновлюється, включаючи нові виявленні вразливості, що дозволяє фахівцям залишатися в курсі останніх загроз та своєчасно вживати необхідних заходів безпеки.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) - це комплексна база знань, розроблена MITRE, яка каталогізує тактику, методи і процедури, що використовуються зловмисниками в реальних кібератаках. Вона слугує цінним ресурсом для розуміння та захисту від методів, що застосовуються суб'єктами загроз на різних етапах життєвого циклу атаки.

Структура ATT&CK складається з декількох матриць, кожна з яких орієнтована на певну платформу або домен, наприклад, корпоративні мережі, мобільні пристрої, промислові системи управління та хмарні середовища. Ці матриці забезпечують структурований спосіб класифікації та документування різних методів і підметодів, що використовуються зловмисниками на етапах розвідки, початкового доступу, виконання, наполегливості, підвищення привілеїв, обходу захисту, доступу до облікових даних, виявлення, бічного переміщення, збору, ексфільтрації, а також на етапах командування і управління атакою.

Використовуючи ATT&CK, фахівці з кібербезпеки можуть отримати уявлення про методи, які використовують сучасні постійні загрози, кіберзлочинці та інші зловмисники. Ці знання допомагають у розробці ефективних стратегій захисту, розширенні можливостей виявлення загроз та реагування на них, а також у покращенні загального стану кібербезпеки.

ATT&CK постійно поповнюється новими методами і спостереженнями з реального світу, що робить його цінним ресурсом для отримання інформації про ландшафт загроз, який постійно змінюється. Він сприяє спільному розумінню поведінки зловмисника, сприяючи співпраці та обміну інформацією в рамках спільноти кібербезпеки.

ATT&CK надає комплексне уявлення про весь спектр тактичних прийомів, що застосовуються зловмисниками на різних етапах операції. Тактика відображає стратегічні цілі або мотиви, які спонукають зловмисника до застосування конкретних методів. Розуміння цих тактик

має вирішальне значення для захисників, щоб ефективно передбачати і пом'якшувати кіберзагрози. Основна матриця Enterprise має 14 етапів та об'єднує всю наявну інформацію.

Тактика Reconnaissance зосереджена на етапі збору життєво важливої інформації, на яку покладаються противники для ефективного планування та визначення масштабів майбутніх операцій. Розвідка може включати пасивний моніторинг відкритих джерел даних, таких як пошкодження веб-сайтів, сховища коду і соціальні мережі, з метою видобутку корисної інформації про ціль. Вона також поширюється на активне сканування, фішинг і соціальну інженерію співробітників, щоб виявити специфічну конфігурацію мережі, облікові дані користувачів та іншу конфіденційну внутрішню інформацію, яка може допомогти в експлуатації.

Перш ніж здійснити операцію, зловмисникам необхідно отримати інфраструктуру та інструменти торгівлі. Resource development охоплює придбання доменів для командування і контролю, компрометації облікових записів користувачів, крадіжки сертифікатів підпису коду і навіть закупівлю наступальних інструментів безпеки на тіньовому ринку. Отримавши ці ресурси, зловмисники можуть розгортати фішингові кампанії, підписувати шкідливе програмне забезпечення для обходу контролю або створювати свою інфраструктуру атак, яка буде використана на наступних етапах.

Отримання такого першого доступу є критично важливим для зловмисників, щоб просунути свій ланцюжок атак. Initial access полягає у використанні вразливостей в системах, що виходять в Інтернет, компрометації ланцюгів постачання, фішингових атаках зі шкідливими вкладеннями або посиланнями і навіть тактиці відключення USB, якщо у них є фізичний доступ. Зловмисники намагатимуться використати численні вектори проникнення доти, доки не вийде запустити код і закріпитися в цільовій мережі.

Отримавши початковий доступ, зловмисники переходять до

executing свого шкідливого коду та корисного навантаження в скомпрометованому середовищі. Це може включати розгортання власного шкідливого програмного забезпечення, використання легальних, але перепрофільованих інструментів, таких як PowerShell, скриптів командного рядка, а також різних шкідливих методів виконання для обходу засобів контролю. Код противника часто переслідує подвійну мету: виявлення, подальше розповсюдження через латеральне переміщення та досягнення інших цілей.

Щоб підтримувати свою присутність протягом тривалих періодів часу, зловмисники використовують механізми persistence, які гарантують, що вони зможуть відновити доступ, незважаючи на переривання. Це включає в себе встановлення бекдорів, перехоплення легітимних програмних процесів, модифікацію ключів запуску реєстру, планування записів завдань та використання інших хитрощів для повторного виконання свого шкідливого коду та корисного навантаження після перезапуску. Постійний доступ є ключовим фактором для того, щоб зловмисники мали час для завершення свого операційного циклу.

Багато з бажаних дій зловмисників вимагають підвищених привілеїв, які виходять за рамки початкового доступу на рівні користувача. Privilege escalation складається з методів використання неправильних конфігурацій, вразливостей і недоліків проектування для отримання більш високих привілеїв, таких як права доступу до системи/кореневого рівня або до певних процесів/даних. Маючи більше прав, зловмисники можуть розгортати руткіти, отримувати доступ до захищених сховищ даних, завантажувати драйвери ядра та повністю контролювати систему.

У процесі своєї діяльності супротивники повинні діяти непомітно і обходити засоби захисту, щоб уникнути виявлення та превентивного реагування. Defence evasion передбачає маскування їхньої інфраструктури, наприклад, системи управління, за допомогою нестандартних протоколів, а також маскування/шифрування їхнього

шкідливого програмного забезпечення, скриптів і комунікацій. Супротивники також безпосередньо виводять з ладу або втручаються в роботу засобів захисту, коли це можливо.

Закріпившись, зловмисники часто намагаються отримати доступ до облікових даних, щоб полегшити подальше переміщення і підвищити свої привілеї в середовищі. Credential access може включати скидання облікових даних з пам'яті, реєстрацію натискань клавіш, грубий перебір або використання неналежного управління обліковими даними, наприклад, багаторазового використання паролів. Отримання легітимних облікових даних маскує дії зловмисників за допомогою довіреного доступу і забезпечує стійкість шляхом створення нових облікових записів. Дійсні облікові дані також є вектором для обходу засобів контролю, які агресивно обмежують поведінку невідомих/ненадійних процесів.

Перед тим, як повністю скористатися доступом і просунутися вглиб мережі, супротивник повинен вжити заходів для того, щоб зрозуміти ситуацію за допомогою discovery дій. Це включає такі методи, як перегляд даних конфігурації системи/мережі, перерахування користувачів/груп, перегляд файлових систем і запити до баз даних, щоб визначити ресурси і виявити цінні цілі, що відповідають їхній місії. Зловмисники використовують комбінацію вбудованих команд, скриптів і спеціальних інструментів для всебічного виявлення та орієнтації в скомпрометований мережі.

Щоб розширити свій оперативний простір і отримати доступ до цінних активів, необхідних для досягнення своїх кінцевих цілей, противники застосовують методи lateral movement. Це включає в себе доступ до віддалених систем за допомогою викрадених облікових даних, проходження через кілька систем, розгортання інструментів віддаленого доступу, використання неправильних конфігурацій та використання спільних ресурсів/засобів, таких як віддалене керування PowerShell. Lateral movement дозволяє зловмисникам розпорошуватися по мережі, поступово збільшуючи свій доступ і контроль, щоб врешті-решт знайти

намічені ними цілі.

Противник намагається зібрати дані, що становлять інтерес для його мети. Collection складається з методів, які супротивник може використовувати для збору інформації та визначення джерел, які мають відношення до досягнення його цілей. Поширеними цілями є файли на різних носіях, дані браузерів, аудіо- та відеозаписи, електронна пошта та інші сховища конфіденційних даних. Типові методи збору включають створення знімків екрану, дамп пам'яті процесів, реєстрацію натискань клавіш, даних, експортованих з баз даних, перегляд резервних копій або місць, де збираються дані.

Противник намагається встановити зв'язок зі скомпрометованими системами, щоб контролювати їх. Command and Control складається з методів, які дозволяють противнику спілкуватися з системами, що знаходяться під його контролем. Вони часто намагаються злитися зі звичайним трафіком, щоб уникнути виявлення. Зловмисники можуть використовувати зашифровані канали, модифікувати реалізацію протоколів або використовувати інструменти віддаленого адміністрування і сервіси, які вже присутні в цільовій мережі. Ефективний C2 має вирішальне значення для зловмисників, щоб зберігати контроль, віддавати вказівки та фільтрувати дані зі свого зловмисного плацдарму.

Зловмисник намагається викрасти дані. Зібравши дані, зловмисники застосовують методи exfiltration, щоб вилучити і викрасти цю інформацію зі скомпрометованої мережі. Це часто передбачає пакування даних за допомогою стиснення та шифрування, щоб приховати їхній вміст під час передачі. Типові шляхи витоку включають перехоплення існуючого з'єднання, створення нового кодованого каналу або видалення даних вручну. Для уникнення виявлення за допомогою квот/порогів на передачу даних можуть використовуватися обмеження розміру.

Противник намагається маніпулювати, перервати або знищити ваші системи та дані. Impact складається з методів, спрямованих на порушення доступності та порушення цілісності шляхом маніпулювання

бізнес-процесами, послугами та операційними технологіями. Знищення даних шляхом стирання, фальсифікації або шифрування є поширеними методами впливу. У деяких випадках процеси можуть виглядати нормальними, але вони були підірвані для прихованого досягнення цілей супротивника. Вплив може бути основною метою або використовуватися як відволікаючий маневр/прикриття для окремих порушень.

Революційність Mitre ATT&CK полягає у тому, що вона відповідає відразу на два питання: «Що хоче зробити зловмисник?» та «Як він цього досягає?». Перевагою перед більш традиційними класифікаціями також є зручна візуалізація, що значно полегшує роботу. Проте, головним недоліком Mitre є її неоднозначність. Одна й та сама атака через матрицю Mitre може бути описана кількома різними способами.

Революційний аспект MITRE ATT&CK полягає в тому, що він стисло відповідає на два критично важливих питання: «Чого хоче досягти противник?» і «Як він це робить?». Ця унікальна структура забезпечує цінний контекст, поєднуючи тактику зловмисника і конкретні методи, що використовуються для її досягнення, в єдиній базі знань. Ключовою перевагою є зручна матрична візуалізація, що значно полегшує розуміння і аналіз поведінки загроз. Однак, помітним недоліком є її неоднозначність - одна й та сама атака може бути описана за допомогою ATT&CK у декілька способів, з використанням різних комбінацій тактик і методів. Незважаючи на цей недолік, MITRE ATT&CK слугує безцінним ресурсом для спільноти кібербезпеки, пропонуючи структурований погляд на тактику, методи і процедури реального супротивника, що дозволяє краще виявляти загрози, запобігати їм і підвищувати загальну обороноздатність.

2.2.1 Кількісна метрика IOC

У [1] було розроблено алгоритм, який визначає рівень захищеності організації, надаючи загальне цілісне уявлення про стан безпеки організації. Визначення метрики безпеки є однією з найважливіших задач

у сфері безпеки. При визначенні метрики безпеки враховується безліч параметрів. Поєднання різних моделей і підходів для оцінки ефективності роботи галузі дозволяє створити систему контролю інформаційної безпеки, проте для цього потрібно вирішити кілька проблем. Важливими завданнями є розробка архітектурного плану функціонування організації, формулювання узагальненого представлення різних моделей і методик, класифікація та визначення системи показників для моніторингу подій процесів, а також формалізація принципів вирішення проблем прийняття рішень щодо забезпечення безпеки. Вирішення цих завдань дозволить створити систему управління безпекою, яка включає елементи моніторингу та прогнозування функціонування організації, що дозволить відслідковувати вплив процесів при зміні подій та показників. Ідея полягає в створенні всебічної системи, яка використовує методи з відомої матриці MITRE ATT&CK для оцінки ризиків та впливу, який вони створюють. Результатом є загальний рейтинг оцінки ризиків організації за кожним методом.

Терміни Impact і Exploitability використовуються для оцінки ризику і складності кібератак. Impact вимірює потенційну шкоду для середовища користувача в разі успіху атаки, в той час як Exploitability відноситься до складності, з якою стикається зловмисник при виконанні атаки. Ця система може бути використана для класифікації різних кібератак на основі їхньої потенційної шкоди та рівня навичок, необхідних для їхнього здійснення.

Відповідно до Common Vulnerability Scoring System (CVSS), ми можемо визначити базовий бал, оцінивши вплив та можливість використання методів з матриці ATT&CK. Це дозволяє нам систематично візуалізувати вплив цільових методів на основі таких факторів, як вектор атаки, складність, масштаб, вимоги до привілеїв, необхідна взаємодія з користувачем, а також метрика Impact, що охоплює вплив на конфіденційність, цілісність та доступність. Ці показники можна зіставити з первинними маркерами низького, середнього та високого рівнів впливу та відповідними балами зловмисності. Кількісно оцінюючи

вплив та можливість використання методів ATT&CK за допомогою цієї методології, ми отримуємо уявлення про їхню потенційну серйозність та шляхи пом'якшення наслідків.

Для побудови рейтингової системи, заснованої на декомпозиції структурних тактик на різні методи, було створено основу для вимірювання та оцінки різних векторів атак для кожного рівня в певний момент часу. Це передбачає формулювання методу генерування оцінки захисту на основі змодельованих оцінок атак на цільове підприємство, які оцінюються за загальною кількістю тактик і методів. Це рівняння вимагає згортки показників, у нашому випадку, Impact та Exploitability, щоб забезпечити швидку генерацію балів у будь-який момент часу.

Початковим кроком для формалізації рівняння є адитивна згортка з постійними ваговими коефіцієнтами для окремих покажчиків, що дозволяє нам оцінити узагальнений показник ефективності для кожного методу, щоб знайти оцінку захисту (Protection Score) системи. Далі ми зважуємо кожну методику за трьома параметрами, а саме: Високий, Середній та Низький. Зрештою, було присвоєно значення цим параметрам, використовуючи шкалу від 0 до 10. Крім того, наступне твердження є справедливим для оцінки рівня захисту кожного методу: Оцінка захисту пропорційна до Exploitability, а оцінка захисту обернено пропорційна до Impact. (a) Збільшення Exploitability техніки є збільшенням Protection Score, оскільки це відображає зусилля, необхідні для обходу систем захисту / захисні механізми. (b) Збільшення Impact технології призводить до зменшення Protection Score, оскільки це відображає ризик і шкоду, яку технологія завдає середовищу користувача.

Оцінка захисту P для окремої методики розраховується як:

$$P = \frac{(\frac{E}{a} - 5)^3 - (\frac{I}{a} - 5)^3 + 100}{2},$$

де E - вага експлуатаційної придатності (висока/середня/низька), I - вага

удару (висока/середня/низька), a - константа коригування графіка = 1.1

Для отримання ефективного показника Protection Score для кількох методик ($P_{totalscore}$), використаних під час оцінювання, потрібно використати зважене середнє арифметичне значення:

$$P_{totalscore} = \frac{\sum_{i=1}^{n} p_i * w_i}{\sum_{i=1}^{n} w_i},$$

де p_i - оцінка захисту i-го методу, w_i - вага, присвоєна категорії захисту (дуже високий/високий/середній/низький/дуже низький).

Таким чином, використовуючи наведені вище формули, можемо успішно розрахувати оцінку рівня захисту для однієї методики або групи методик.

Висновки до розділу 2

У цьому розділі представлено модель оцінки IOC, яка враховує довіру до джерела та часовий спад значущості IOC. Модель використовує логістичну функцію для нормалізації значень довіри та імпульсів, а також функцію зменшення для моделювання зменшення довіри з часом. Крім того, розглянуто децентралізований підхід з використанням технології блокчейн та протоколу консенсусу PoRep для вирішення проблеми різної якості джерел IOC.

Також обговорюються CVE та MITRE ATT&CK як важливі ресурси для розуміння вразливостей та методів, що використовуються зловмисниками. Нарешті, запропоновано кількісну метрику для оцінки рівня захищеності організації на основі методів MITRE ATT&CK, враховуючи вплив та експлуатаційну придатність кожного методу.

3 МОЖЛИВІ АТАКИ НА БЛОКЧЕЙН, ЩО ВИКОРИСТОВУЄТЬСЯ В МОДЕЛІ КІЛЬКІСНОЇ ОЦІНКИ IOC

3.1 Атака подвійної витрати

Суть атаки подвійної витрати (Double Spending Attack) [6] полягає в тому, що зловмисник намагається дві майже послідовні транзакції з двома різними вузлами мережі.

Нехай, зловмисник в блоці $B[n]$, де n - номер блоку в мережі, виконує транзакцію, в якій відправляє гроші продавцю за товари або послуги. Продавець отримує гроші і відправляє товар покупцеві. Після того, як покупець отримує товар, зловмисник намагається побудувати альтернативний блок $B[n]$, який вказує на попередній блок $B[n-1]$. При побудові цього альтернативного блоку ті ж самі кошти надсилаються на іншу адресу або гаманець як оплата іншому постачальнику за товари або послуги.

Щоб мережа блокчейн прийняла новостворений підроблений блок, зловмисник намагається додати більше блоків до альтернативного блоку. Якщо зловмиснику вдасться створити альтернативну гілку блокчейну, довшу за справжню, то, згідно з правилами протоколу майнінгу, його гілка буде вважатися дійсним ланцюжком. Отже, що чим більша частка ресурсів зловмисника, тим вищі його шанси на успішне виконання цієї атаки подвійних витрат. Зокрема, якщо частка ресурсів зловмисника перевищує 50%, ймовірність успішної атаки стає рівною 1.

Зловмисник публікує альтернативну гілку, якщо вона дорівнює або перевищує кількість блоків у чесному ланцюжку. Чим більше обчислювальних потужностей або криптовалют у зловмисника в системі, тим вищі шанси здійснити таку атаку.

Щоб запобігти цій атаці, необхідна достатня кількість блоків

підтвердження, щоб зловмисник не зміг наздогнати чесних майнерів.

Стійкість до атаки Double Spend

Нехай r - спільна репутація, r_m - спільна зловмисна репутація, r_h - спільна репутація чесних майнерів, z - кількість чесних блоків, k - кількість нечесних блоків. ξ - кількість таймслотів, які належать зловмиснику до моменту, поки майнери будуть мати z блоків.

Ймовірність того, що буде вибрано рівно k зловмисних блоків:

$$P(\xi = k) = C^k_{z+k-1} p_h^z p_m^k, \tag{3.1}$$

де $p_h = \frac{r_h}{r}$, $p_m = \frac{r_m}{r}$, $p_h > p_m$, $p_h + p_m = 1$.

Отже, атака відбувається у два етапи. На першому етапі чесні майнери будують основний ланцюг з блоків підтвердження, тоді як зловмисник намагається створити альтернативний, довший ланцюг. Якщо на першому етапі зловмиснику не вдалося побудувати довший ланцюг, починається другий етап, під час якого зловмисник намагається зрівняти свій альтернативний ланцюг з основним, прагнучи наздогнати чесних майнерів. Після того, як чесні майнери знайшли z блоків, ймовірність успіху зловмисників у цій атаці визначається як:

$$\begin{aligned} P(\texttt{успішна атака}) &= \sum_{k=z}^{\infty} C^k_{z+k-1} p_h^z p_m^k + \sum_{k=0}^{z-1} C^k_{z+k-1} p_h^z p_m^k \left(\frac{p_m}{p_h}\right)^{z-k} = \\ &= 1 - \sum_{k=0}^{z-1} C^k_{z+k-1} p_h^z p_m^k + \sum_{k=0}^{z-1} C^k_{z+k-1} p_h^k p_m^z = \\ &= 1 - \sum_{k=0}^{z-1} C^k_{z+k-1} (p_h^z p_m^k - p_h^k p_m^z). \end{aligned} \tag{3.2}$$

На графіку 3.1 можна побачити, як зменшується ймовірність успіху атаки з подвійною витратою зі збільшенням кількості перевірочних блоків

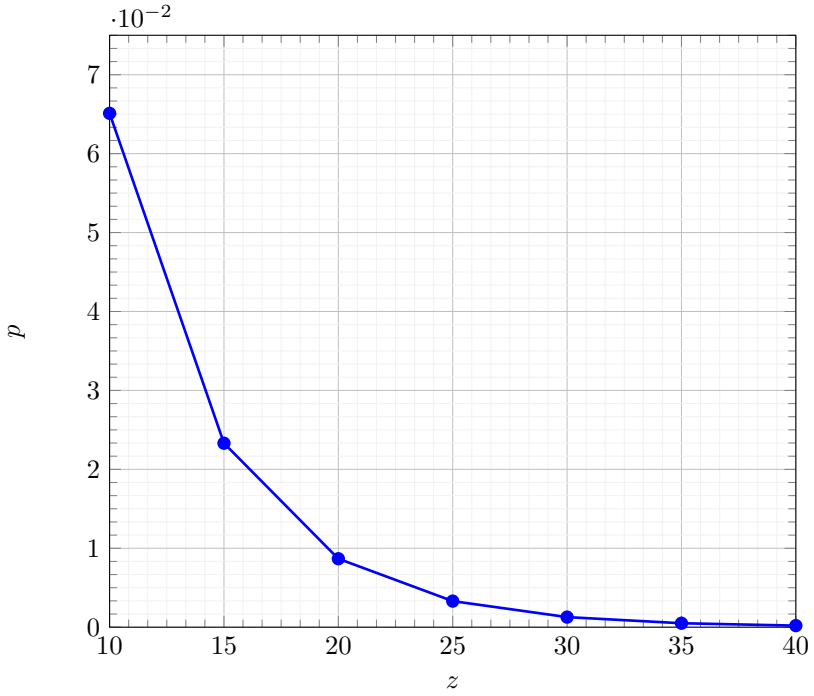

Рисунок 3.1 – Графік імовірності успішності атаки подвійної витрати від заданого z при $p_m = 0.3$

z, коли ймовірність того, що зловмисник згенерує блок p_m, фіксована на рівні 0.3. При низьких значеннях z ймовірність успішної атаки подвійної витрати досить висока, оскільки зловмиснику з імовірністю 30% вдається генерувати альтернативні блоки та створювати більш довгий ланцюжок, ніж основний. Однак зі збільшенням z ймовірність успіху стрімко падає, слідуючи за кривою, яка швидко спадає до нуля.

Таким чином, графік ілюструє основний баланс між безпекою та часом підтвердження в мережах блокчейн. Вище значення z забезпечує більший захист від атак подвійних витрат, але вимагає більшого часу очікування для того, щоб транзакції вважалися повністю підтвердженими. І навпаки, нижче значення z дозволяє швидше підтверджувати транзакції, але збільшує ризик подвійних витрат.

3.2 Атака Denial of Service

Майнери відіграють вирішальну роль в ефективному функціонуванні блокчейн мереж, оскільки вони відповідають за створення нових блоків та підтвердження транзакцій. Тому їхня нормальна робота є критично важливою для безпечності та стабільності всієї системи. У зв'язку з цим, майнер може розглядатися як зловмисний вузол, якщо він навмисно уникає участі у процесі генерації блоків під час свого раунду або не виконує інші обов'язкові функції у мережі. Такі дії можна трактувати як атаку, спрямовану на порушення нормальної роботи блокчейну.

Зловмисна поведінка майнера може виражатися у відмові від майнінгу блоків під час свого раунду генерації, ігноруванні вузлами правил консенсусу мережі або навмисному створенні недійсних блоків, намаганнях маніпулювати мережею шляхом атак, таких як подвійна витрата коштів або цензурування транзакцій, а також будь-яких інших діях, що навмисно перешкоджають належному функціонуванню блокчейну. Важливо відзначити, що реакція мережі на такі зловмисні дії майнерів може різнитися залежно від конкретного блокчейн протоколу. Деякі мережі можуть передбачати механізми покарання, такі як штрафи або виключення зловмисних майнерів. В інших випадках, така поведінка просто призводить до зниження ефективності роботи всієї мережі.

Стійкість до атаки Denial of Service

Нехай чесний майнер з якихось причин не виконує свої обов'язки щодо генерації блоків або не бере активної участі у функціоналі мережі, його можна розглядати як потенційно зловмисний вузол. Для вирішення цієї проблеми у багатьох блокчейн протоколах передбачено механізм голосування, за яким такий майнер може бути виключений з мережі.

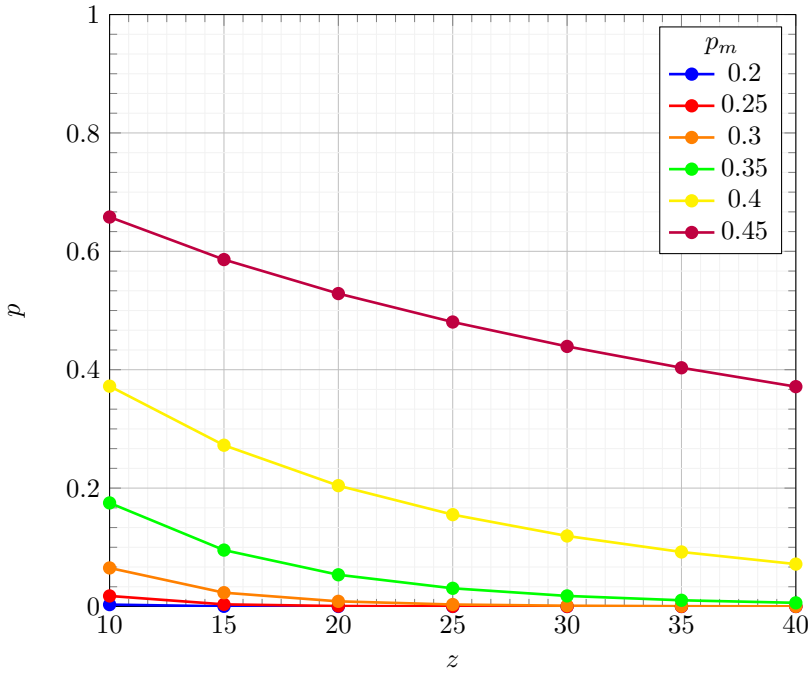

Рисунок 3.2 – Графік імовірності успішності атаки подвійної витрати від заданого z та зменшення імовірності p_h та збільшення p_m

Якщо чесний майнер виключається, тоді частка чесних майнерів зменшується. Відповідно, частка під контролем зловмисників p_m збільшується. Це полегшує для зловмисників здійснення атаки подвійної витрати, оскільки їм потрібно контролювати меншу відносну частку обчислювальної потужності порівняно з чесними майнерами.

Таким чином, виключення неактивних або зловмисних майнерів призводить до збільшення частки p_m геш-потужності під контролем інших зловмисників. Це дозволяє звести потенційну атаку Denial of Service до більш простої атаки подвійної витрати для зловмисників. Відповідно, стійкість блокчейн мережі до такої атаки зменшується.

На наведеному графіку 3.2 представлено залежність ймовірності успіху атаки з подвійною вартістю від параметра z при різних значеннях ймовірності генерації блоку зловмисником p_m. Чітко видно, що зі збільшенням p_m крива ймовірності успіху атаки зміщується вгору. Це означає, що при більш високих значеннях p_m, коли зловмисник має більші шанси згенерувати наступний блок у ланцюжку, ймовірність

успішної реалізації атаки з подвійною вартістю зростає. Отже, чим вища частка обчислювальної потужності контролюється зловмисником, тим вища загроза такої атаки на блокчейн мережу.

3.3 Атака Eclipse

Зловмисник намагається ізолювати вузол або групу вузлів, щоб перешкодити цільовим вузлам отримати поточне уявлення про мережеву активність і стан блокчейну. Атака Eclipse спрямована на порушення здатності вузла отримувати актуальну інформацію про стан блокчейну та транзакції, що відбуваються в мережі. Ізольований вузол буде змушений покладатися виключно на зловмисні дані, надані атакуючим. Це дозволяє зловмиснику здійснювати інші атаки, таку як атаку подвійної витрати, оскільки ізольований вузол не зможе перевірити достовірність наданих даних з іншими вузлами в мережі.

Стійкість до атаки Eclipse

Нехай зловмисник – це зловмисний вузол, який знаходиться в стратегічній позиції в мережі і не пересилає транзакції та/або блоки наступним вузлам, намагаючись заперечити поточну версію блокчейну для інших вузлів.

Ця атака може бути пом'якшена в класичних мережах шляхом встановлення надлишкових шляхів між вузлами мережі. У нашій пропозиції припускається, що всі учасники з'єднані між собою як мінімум двома резервними шляхами в мережі.

На графіку 3.3, який аналогічний до графіку 3.2 попередньої атаки, можна побачити, що зі збільшенням p_m криві ймовірності успіху атаки зміщуються вгору. Це означає, що чим більша частка обчислювальних потужностей контролюється зловмисником, тим вищі його шанси успішно

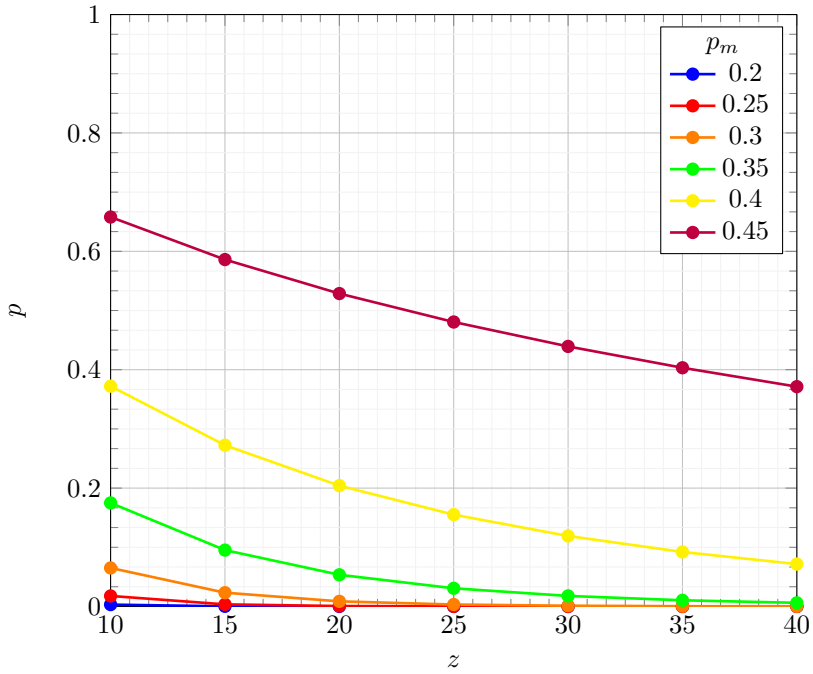

Рисунок 3.3 – Графік імовірності успішності атаки подвійної витрати від заданого z та зменшення імовірності p_h та збільшення p_m

реалізувати цей тип атаки на блокчейн мережу. Загальний висновок залишається тим самим - зростання p_m підвищує загрозу безпеці мережі від такого роду атак.

3.4 Атака 51%

Зловмисник повинен контролювати значну частину мережі, перш ніж впливати на механізм консенсусу. Атака, відома як «атака 51%», вимагає, щоб користувач або група зі спільними інтересами контролювала щонайменше 51% потужності мережі для перевірки блоків.

Стійкість до 51% атаки

Нехай p-ймовірність успіху нечесного майнера, відповідно $q = 1 - p$ - ймовірність успіху чесного майнера. Нехай це буде в нас оцінками зверху. А щоб отримати оцінку ставки нечесного майнера, яка буде після певної

кількості його успіхів.

Тоді цей процес описується схемою Бернуллі. Нехай $\xi_i, i \geqslant 1$, де

$$\xi_i = \begin{cases} 1, & \text{за імовірністю p,} \\ -1, & \text{за імовірністю q.} \end{cases}$$

Введемо випадкові величини:

$$S_0 = 0, S_n = \sum_{i=1}^{n} \xi_i \tag{3.3}$$

$$S_0^- = 0, S_n^- = \sum_{i=1}^{n} (-\xi_i V 0) \tag{3.4}$$

$$S_0^+ = 0, S_n^+ = \sum_{i=1}^{n} (\xi_i V 0) \tag{3.5}$$

S_0^+, $n = 0,1,...$ – кількість успіхів нечесного майнера;

S_0^-, $n = 0,1,...$ – кількість невдач нечесного майнера;

Тоді при $\lim\limits_{n\to\infty} p_n = 0$, $\lim\limits_{n\to\infty} np_n = l$, $l \geq 0$ $\lim\limits_{n\to\infty} P(\text{кількість успіхів} = m) = e^{-l} \cdot \frac{l^m}{m!}$.

3.5 Атака Selfish Miner

Зловмисник вибирає, які транзакції майнити, навмисно ігноруючи інші транзакції. атака полягає в тому, що пул зловмисних майнерів приховує знайдені блоки, створюючи приватну гілку блокчейну. Коли приватна гілка стає достатньо довгою, майнери публікують її, отримуючи перевагу в винагороді. Якщо «егоїстичний» майнер знаходить блок, він приховує його і починає майнити на цій приватній гілці. Якщо він знаходить наступний блок, атака успішна. Якщо ж чесний майнер знаходить блок на тій же гілці, «егоїстичний» майнер публікує свій блок, починаючи конкуренцію. «Егоїстичний» майнер отримує винагороду, якщо знаходить блок після свого блоку. Негативний результат для нього -

це коли чесний майнер знаходить блок після блоку чесного майнера.

Стійкість до атаки Selfish Miner

Нехай зловмисник вибирає транзакції для майнінгу та ігнорує інших у своєму раунді майнінгу. Атака повинна тривати один раунд через ротацію майнінгу серед майнерів. Наступний легальний майнер в ротації буде видобувати найстаріші транзакції. Як тільки егоїстичний майнер буде виявлений, судді знизять його репутацію та/або проголосують за вигнання нападника.

3.6 Атака Impersonation

Зловмисник намагається отримати інформацію про конфігурацію або видати себе за майнера.

Стійкість до атаки Impersonation

Нехай зловмисник – це зловмисний вузол, який намагається видати себе за інший вузол. Його метою є модифікувати, пошкодити або створити транзакцію та/або блок, видаючи себе за інший вузол мережі.

Зловмисник може спробувати змінити або пошкодити транзакцію, перш ніж переслати її наступним вузлам. Однак це може статися лише з мізерно малою ймовірністю успішної підробки криптографічного підпису. Атаки, які шукають інформацію про конфігурацію, зменшуються завдяки шифруванню конфіденційної інформації. Таким чином, зловмисникам необхідно отримати приватний ключ передбачуваного одержувача. Крім того, запропонована модель дозволяє проводити аудит всіх минулих транзакцій. Тому, якщо зловмисник спробує модифікувати блокчейн за допомогою викраденої пари ключів, ця спроба буде зафіксована в

журналі. Після виявлення зловмисника, вкрадені пари ключів можна легко видалити з мережі, відновивши безпечну роботу мережі та уникнувши подальшої шкоди.

Висновки до розділу 3

У цьому розділі розглянуто різні типи атак на блокчейн, що використовується в моделі кількісної оцінки IOC. Розглянуто атаку подвійної витрати, атаку відмови в обслуговуванні, атаку Eclipse, атаку 51% та атаку Selfish Miner. Для кожної атаки обговорюється її принцип дії, а також механізми стійкості блокчейну до цих атак.

ВИСНОВКИ

У ході даної роботи був проведений аналіз опублікованих джерел за тематикою індикаторів компрометації, протоколів консенсусу Proof-of-history та Proof-of-authority, а також методів кількісної оцінки якості індикаторів компрометації (IOC). В результаті аналізу було виявлено, що існуючі методи кількісної оцінки IOC не враховують вплив часу на їхню актуальність та потребують централізованих систем управління, що робить їх вразливими до кібератак.

У зв'язку з цим, було запропоновано децентралізований підхід до кількісної оцінки IOC з використанням технології блокчейн та протоколу консенсусу Proof-of-Reputation (PoRep). Цей підхід дозволяє врахувати вплив часу на актуальність IOC, а також забезпечує більш високу стійкість до кібератак завдяки децентралізованому характеру системи.

Була розроблена модель та методика кількісної оцінки IOC, яка враховує вплив часу та використовує блокчейн-технології. Модель включає динамічний рейтинг IOC, який кількісно оцінює надійність кожного учасника, що надає IOC в мережу. Рейтинг IOC користувача з часом поступово знижується, якщо не спостерігається подальшої зловмисної активності, імітуючи природний занепад застарілих показників.

Для забезпечення безпеки запропонованої моделі було проведено аналіз стійкості протоколів Proof-of-history та Proof-of-authority до відомих атак на протоколи Proof-of-Stake (PoS) типу. В результаті аналізу було виявлено, що протоколи PoH та PoA мають високу стійкість до атак подвійної витрати, Denial of Service, Eclipse, 51%, Impersonation та Selfish Miner.

Графіки 3.1, 3.2, 3.3 ілюструють залежність ймовірності успіху атаки подвійної витрати від кількості перевірочних блоків z та ймовірності генерації блоку зловмисником pm. З графіків видно, що зі

збільшенням z та зменшенням pm ймовірність успіху атаки зменшується.

Запропонована модель та методика кількісної оцінки IOC з використанням блокчейн-технологій може бути використана для підвищення ефективності систем виявлення вторгнень та захисту інформаційних систем від кібератак.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Hardik Manocha та ін. «Security Assessment Rating Framework for Enterprises using MITRE ATT&CK Matrix». Англ. В: (2021). URL: https://arxiv.org/abs/2108.06559.

[2] M. T. de Oliveira та ін. «Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications». Англ. В: *Comput. Netw.* 179 (2020), с. 107367. DOI: 10.1016/j.comnet.2020.107367. URL: https://doi.org/10.1016/j.comnet.2020.107367.

[3] Vipul Saini. *ConsensusPedia: An encyclopedia of 30+ consensus algorithms*. Англ. URL: https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f.

[4] V. Tkach та ін. «Indicators of compromise confidence scoring method». Англ. В: (2023). URL: https://idaacs.digital/wp-content/uploads/2023/09/IDAACS23_PROCEEDINGS_VOL_1_new_3.pdf.

[5] Anatoly Yakovenko. «Solana: A new architecture for a high performance blockchain v0.8.13». Англ. В: (2022). URL: https://solana.com/solana-whitepaper.pdf.

[6] Л. В. Ковальчук, А. М. Кудін та Н. В. Кучинська. *Вступ до технології блокчейн та криптовалют. Частина 1. Теоретичні засади функціонування блокчейн-технологій.* URL: http://ela.kpi.ua/handle/123456789/49232. Kyiv: КПІ ім. Ігоря Сікорського, 2022, с. 142.

ДОДАТОК А ТЕКСТИ ПРОГРАМ

A.1 main.ipynb

```
from scipy.special import comb
from math import pow
import pandas as pd
import numpy as np

def p_successful_attack(z, p):
  r = 1
  for k in range(z):
    r -= comb(z+k-1, k)*(pow(p[1], z)*pow(p[0], k) - pow(p[0], z)*pow(p[1], k))
  if r > 1:
    return 1
  else:
    return r

# Double Spend Attack
p = (0.3, 0.7)
z = [10, 15, 20, 25, 30, 35, 40]

data_success = {'z': z, 'probability': [p_successful_attack(zi, p) for zi in z]}
df_success = pd.DataFrame(data_success)

print(f"Probability of success (p_m = {p[0]}):")
df_success
# Denial of Service ma Eclipse
p = [0.2, 0.25, 0.3, 0.35, 0.4, 0.45]
z = [10, 15, 20, 25, 30, 35, 40]

data_list = [
    {'z': zi, 'p_m': pi, 'probability': p_successful_attack(zi, (pi, 1 - pi))}
    for zi in z for pi in p
]
data = pd.DataFrame(data_list).pivot_table(index='p_m', columns='z', values='probability')
print(f"Probability of success:")
data
```