ВІДГУК

рецензента – доцента кафедри захисту інформації,
Національного університету "Львівська політехніка",
к.т.н., доцента Совина Ярослава Романовича
на дисертацію
Василишина Святослава Ігоровича
«Розробка методу використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain»,
подану на здобуття наукового ступеня доктора філософії за спеціальністю
125 «Кібербезпека та захист інформації»
(галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації.

Як проактивний захисний механізм, honeypot стає незамінним інструментом для забезпечення безпеки мережі в таких широких додатках, як Інтернет речей (IoT), бездротові сенсорні мережі (WSN), транспортні мережі тощо. Завдяки проактивності та контролю, honeypot може залучити зловмисника до взаємодії з підробленими системними ресурсами, що запобігає атаці на цінні ресурси. У порівнянні з традиційними методами, включаючи, але не обмежуючись, брандмауер і систему виявлення вторгнень (IDS), honeypots повністю скидають пасивність у домені захисту мережі. У зв'язку з цим, приманки привернули широку увагу серед сил кібербезпеки. Спроби зловмисників зламати системи безпеки зростають з кожним днем. Зловмисники використовують такі інструменти, як SubSeven, Nmap і LoftCrack, щоб сканувати, ідентифікувати, досліджувати та проникати в корпоративні системи.

Для запобігання такому несанкціонованому доступу до корпоративних мереж встановлюються брандмауери. Однак брандмауери не можуть запобігти атакам, що надходять з інтранету. Система виявлення вторгнень (IDS) перевіряє мережевий трафік і визначає експлойти та вразливості; вона здатна відображати попередження та реєструвати події. З іншого боку, система запобігання вторгненням намагається запобігти відомим сигнатурам вторгнень і деяким невідомим атакам завдяки знанням про поведінку атак у своїй базі даних. Однак IDS може щодня генерувати тисячі попереджень про вторгнення, деякі з яких є помилковими. Це ускладнює для IDS виявлення та ідентифікацію реальних загроз і захист активів. Таким чином, для розслідування атак, виявлених і повідомлених IDS, потрібне втручання людини. Побудувати мережу, яка базується на основі та засадах технології Blockchain дуже складне завдання та потребує неабияких знань та досвіду в даній сфері. З попереднього твердження випливає й те, що цей процес також не один із найдешевших. Хороші спеціалісти на ринку, які працюють саме в цій сфері дуже дорого обходяться та й до того поки що їх не надто багато. Додаткова складність полягає в тому, що використання готових рішень, наприклад розгалуження від першорівневої мережі, такої як Etherum або Solana, не підходить для реалізації систем захисту інформації, а особливо, якщо говорити про спеціалізовані

системи або об'єкти критичної інфраструктури чи безпеки компанії. Необхідно розробляти свій власний першорівневий Blockchain разом з політиками безпеки, приєднання та від'єднання вузлів (користувачів) до системи, протоколи авторизації та аутентифікації користувачів. У понятті безпеки, коли це стосується важливих та стратегічних об'єктів не повинно бути такого слова, як економія, адже в 80% випадків зловмисник отримує доступ до внутрішньої мережі або успішно проводить DDoS та інші види атак на об'єкти саме через економію на захисті від даної атаки. Решта 20% включає в себе людський фактор, до якого можна зараховувати як і некомпетентність операторів системи (соціальна інженерія), так і її розробників. Однак, поряд з можливостями, які надає Blockchain, необхідно звернути особливу увагу на захист та безпеку учасників мережі, зокрема валідаторів. У сучасному світі різні методи захисту, такі як паролі, біометрія та двофакторна автентифікація через додатки типу Google Authenticator, використовуються на платформах, таких як Binance та Huobi. Проте, на додачу до цих методів, розглядається можливість впровадження NFC-міток для забезпечення ще більш надійнішого захисту та забезпечення надійності Blockchain-мереж.

Дисертаційна робота присвячена вирішенню актуального науково-практичного завдання підвищення ефективності виявлення кіберзлочинів та покращення стійкості захисної системи за рахунок розробки методу використання приманок на основі динамічних атрибутів Blockchain. Це дасть змогу підвищити ефективність захисту комп'ютерних мереж шляхом зменшення навантаження на мережеву інфраструктуру та часу відгуку сервісів для підсилення рівня кіберзахисту інформації в приватних або державних компаніях.

Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри

Дисертаційні дослідження Василишина С.І. виконувалися в межах держбюджетної науково-дослідної роботи «Розроблення та удосконалення методів та засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-комунікаційних мережах» (№ державної реєстрації 0119U101690; терміни виконання - 2019-2022 рр.);

Наукова новизна основних результатів дисертації полягає в розробленні методів використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain:

1. *Вперше розроблено* модель динамічної системи активних програмних приманок, що використовують блокчейн технологію. На відміну від відомих дана модель інтегрує децентралізовані та автоматично оновлювані атрибути пасток, що дало змогу підвищити ефективність захисту мережі шляхом зменшення навантаження на мережеву інфраструктуру та часу відгуку сервісів у випадку атаки.
2. *Набув подальшого розвитку* математичний опис обчислення динамічних атрибутів програмних приманок, який, на відміну від відомих, враховує

динамічні та транс локаційні можливості блокчейн-технології Solana. Це дало змогу змоделювати та оптимізувати розподіл ресурсів мережі за рахунок адаптації до змінних умов, що в результаті сприяло підвищенню ефективності захисту, зокрема забезпеченню швидкого відгуку сервісів під час зовнішніх атак.

3. *Вперше розроблено* метод використання програмних приманок як елементів захисту комп'ютерних мереж з використанням технології Blockchain, на основі розробленої моделі динамічної системи програмних (активних) приманок, яка використовує блокчейн-технологію для підтримки безпеки, прозорості та адаптивності до зовнішніх атак, за рахунок плаваючих хостів в мережі та математичного апарату обчислення динамічних атрибутів програмних приманок. Цей метод, на відміну від відомих унеможливлює здійснення успішної сніфер атаки за рахунок шифрування, захищає від атаки сканування за рахунок динамічного відкривання та закривання портів, підвищує ефективність захищеності від DDoS атак та зберігає інформацію про атаки на систему на блокчейн-платформі, що забезпечує високий рівень збереження даних та гарантує їхню незмінність.

Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна.

Наведені в дисертації результати базуються на кваліфікованому підході до постановки завдань досліджень, логічно правильному обґрунтуванню прийнятих допущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується результатами комп'ютерного моделювання і практичною реалізацією системи динамічних програмних приманок, а також збіжністю з результатами експериментальної верифікації.

Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати.

Наукові результати, отримані автором, можуть бути використані при розробці та побудові новітніх мережевих систем, які використовують технологію Blockchain та програмні приманки в якості активного захисту та для підсилення наявних систем захисту в приватних або державних компаніях

Також їх можна впровадити у навчальний процес у курсі "Безпека мобільних технологій" для студентів спеціальності 125 "Кібербезпека".

Практичне значення одержаних результатів полягає у можливості їх безпосереднього застосування для підсилення наявних систем активного та пасивного захисту.

1. Розроблена модель динамічної системи активних пасток на основі програмних приманок побудованих на системі Blockchain, яка дала змогу в залежності від різних ситуацій моделювання (в залежності від атаки) до 54% підвищити пропускну здатність каналу та до 204% підвищити швидкість

передачі даних під час проведення зовнішніх атак на систему в порівнянні з статичними аналогами.

2. Удосконалення математичного апарату програмних приманок за рахунок додавання та обчислення динамічних атрибутів програмних приманок дало змогу покращити час відгуку сервісів під час атаки типу DDoS на статичні хости, в межах таких значень – MSQL до 34%, NGNIX до 16%, APACHE до 1%, vsFTPd до 13%.

3. Підвищено ефективність захищеності каналів передачі даних у комп'ютерній мережі за рахунку впровадження розробленого методу динамічної системи активних пасток на основі програмних приманок побудованих на технології Blockchain з RSA 2048-бітовим алгоритмом шифрування. Система активних пасток не дозволяє декодувати інформацію без відповідного ключа конфіденційності, що забезпечує захист каналу передачі даних та запобігає витоку даних через перехоплення та розшифрування інформації під час її передачі. Експеримент з сніфер атакою на розроблену модель системи підтвердив ефективність реалізації захисту від перехоплення на основі шифрування.

4. Удосконалення алгоритму визначення та передачі вузлових хостів у системі Blockchain, за рахунок впровадження плаваючих хостів у мережі, підвищило загальну адаптивність мережі щодо реагування на зовнішні атаки. Цей алгоритм, на відміну від відомих, дозволяє системі реагувати на атаки типу сканування та закривати порти доступу реагуючи на зловмисні дії. Результати експерименту під час атаки сканування на відкриті порти дозволили автоматизувати закриття портів, за рахунок зміни основного хоста, що ускладнює збір інформації та можливість доступитись до системи ззовні.

5. Розроблений метод використання програмних приманок, що побудований на основі використання технології Blockchain, вимагає більше ресурсів від нападника для здійснення атаки на мережу: потужності комп'ютерів, серверів з яких здійснюється атака, а також більше фізичного часу, що збільшує час для фахівців з кібербезпеки для реагування та контр дії нападу до 45%. Було проведено однакову кількість атак як на централізовану систему, яка використовує програмні приманки, так і на динамічну систему, яка побудована на розробленому методі. Найбільшу різницю видно не на всіх сервісах: Apache та Nginx динамічної системи зазнають під час атаки майже однакового з центральним аналогом результатів. Однак сервіси Vsftpd та MySQL вимагають використання значно більших ресурсів від нападника, що показує ефективність розробленого методу у плані захисту комп'ютерної мережі. З тридцяти проведених атак розроблена модель успішно заблокувала 50% в той час як централізована всього 13%, що показує покращення захисних можливостей розробленої моделі. Захист децентралізованої моделі мережі під час DDoS атаки вищий на 14%. Захист децентралізованої моделі мережі під час атаки сканування вищий на 44%. Захист децентралізованої моделі мережі під час сніфер атаки вищий на 37%. Загальний захист комп'ютерної мережі побудованої з використанням програмних приманок на основі технології Blockchain вищий на 37% у порівнянні з централізованим аналогом, що є підвищенням глобального рівня захисту комп'ютерної мережі в півтора рази.

Запропоновані в роботі підходи та методи дають змогу суттєво підсилити існуючі системи активного та пасивного захисту інформації в корпоративних та державних підприємствах. Розроблена модель динамічної системи активних програмних приманок, що використовують блокчейн технологію, інтегрує децентралізовані та автоматично оновлювані атрибути пасток, що дає можливість підвищити ефективність захисту мережі шляхом зменшення навантаження на мережеву інфраструктуру та часу відгуку сервісів у разі атаки. Це оптимізує розподіл ресурсів мережі за рахунок адаптації до змінних умов, що в результаті сприяє підвищенню ефективності захисту, зокрема забезпеченню швидкого відгуку сервісів під час зовнішніх атак.

Результати дисертаційної роботи впроваджено у технологічні процеси ТОВ "Н-ІКС СПЕЙС" (м. Львів).

Зауваження по дисертації.

1. У першому розділі в таблиці 1.2. зазначена порівняльна характеристика додатків побудованих на першому рівні Blockchain, однак порівняно всього три додатки, варто було б збільшити вибірку до 5-6 для покращення порівняльної характеристики.
2. Обсяг другого розділу виглядає завеликим, і частину матеріалу доцільно було б винести у додатки, наприклад, починаючи з пункту 2.2.4 значну кількість місця займає код, який варто було б форматувати в додатку, як це зроблено для смарт-контракту.
3. Розділ 4.3 варто було б об’єднати з розділом 4.2. Інформація в даному розділі – це табличне представлення тих самих даних отриманих у попередньому розділі.
4. Наявні незначні граматичні помилки та одруки.

Слід відзначити, що вказані зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Висновок

Дисертація Василишина Святослава Ігоровича на тему "Розробка методу використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain" є завершеною науковою працею, у якій розв’язано конкретне наукове завдання – підвищення ефективності захисту комп’ютерних мереж та покращення стійкості захисної системи без втрати швидкодії мережевої інфраструктури за рахунок розробки системи приманок на основі динамічних атрибутів блокчейну для підсилення рівня кіберзахисту інформації, що має важливе значення для галузі знань 12 "Інформаційні технології". Дисертація відповідає вимогам наказу МОН України № 40 від 12.01.2017 р. "Про затвердження вимог до оформлення дисертації" (зі змінами, внесеними згідно з Наказом МОН України № 759 від 31.05.2019р.), "Порядку присудження ступеня доктора філософії та скасування рішення спеціалізованої

вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії", затвердженого постановою Кабінету Міністрів України від 12.01.2022 р. № 44 (зі змінами внесеними згідно з постановою Кабінету Міністрів України № 341 від 21.03.2022 р.), а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 “Кібербезпека та захист інформації”.

Офіційний рецензент
Кандидат технічних наук, доцент,
Доцент кафедри захисту інформації
Національного університету
“Львівська політехніка” Ярослав СОВИН

Підпис к.т.н., доцента Совина Я.Р. засвідчую.

Вчений секретар
Національного університету
“Львівська політехніка”
к.т.н., доцент Роман БРИЛИНСЬКИЙ