РЕЦЕНЗІЯ

Кандидата технічних наук, старшого викладача кафедри захисту інформації

Партики Андрія Ігоровича

на дисертацію

Журавчака Даниїла Юрійовича

«Удосконалення методів виявлення програм-вимагачів в режимі реального часу»

подану до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека»

(галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації.

Актуальність дисертаційної роботи Д.Ю. Журавчака "Удосконалення методів виявлення програм-вимагачів в режимі реального часу" зумовлена стрімким зростанням кількості та складності кібератак з використанням програм-вимагачів. Ці шкідливі програми завдають значних фінансових та репутаційних збитків організаціям усіх видів, включаючи державні установи, медичні заклади, підприємства та освітні установи. Швидкий розвиток та еволюція програм-вимагачів, їх використання у кібервійнах, особливо в контексті війни в Україні, підкреслюють їхню небезпеку та вимагають розробки нових, більш ефективних методів виявлення та протидії.

У дисертації запропоновано інноваційний підхід до виявлення програм-вимагачів, який базується на інтеграції технології eBPF (розширений фільтр пакетів Берклі) та моделей машинного навчання. Цей підхід дозволяє здійснювати моніторинг системних подій у режимі реального часу та виявляти підозрілу активність на ранніх стадіях, що є критично важливим для запобігання атакам та мінімізації їх наслідків.

Дисертація пропонує комплексний підхід до вирішення проблеми, враховуючи різні аспекти кібербезпеки, від моніторингу системних подій до аналізу мережевого трафіку та поведінки процесів. Розроблені автором методи

та інструменти мають практичну цінність для фахівців з кібербезпеки та можуть бути використані для підвищення рівня захисту інформаційних систем.

Таким чином, актуальність дисертації Д.Ю. Журавчака підтверджується її спрямованістю на вирішення нагальної проблеми кібербезпеки, важливістю розробки нових методів захисту від програм-вимагачів та потенційним внеском у підвищення рівня кібербезпеки як в Україні, так і в світі.

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

Дисертаційні дослідження 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.); Окремі частини роботи виконано в межах держбюджетної науково-дослідної роботи: «Дослідження стійкості біометричних систем автентифікації до атак із застосуванням технології клонування голосу на основі глибинних нейронних мереж» (№ держреєстрації 0124U000407).

Наукова новизна основних результатів дисертації полягає у тому, що:

Наукова новизна полягає у тому, що:

1. Вперше розроблено модель інтегрованої системи збору даних для виявлення вірусів-вимагачів, що об'єднує застосування eBPF для моніторингу системних викликів, файлової та криптографічної активності, аналізу мережевого трафіку та процесів. Ця система забезпечує унікальний набір даних (features), які використовуються для ефективного ідентифікування потенційних загроз в режимі реального часу.

2. Вперше запропоновано комплексну модель класифікації вірусів-вимагачів з використанням ансамблю дерев рішень та випадкового лісу, що дозволяє з високою точністю розрізняти "безпечні" та "небезпечні" програми на основі аналізу складних поведінкових шаблонів та криптографічної активності.

3. Вперше запропоновано методологію застосування глибоких нейронних мереж для ідентифікації складних шаблонів у даних зібраних модулями eBPF, що представляють поведінку вірусів-вимагачів, забезпечуючи новий рівень точності виявлення невідомих або еволюціонованих загроз.

4. Отримали подальший розвиток методи виявлення кіберзагроз за допомогою аналізу мережевого трафіку з використанням eBPF, що значно підвищує швидкість та точність ідентифікації потенційних атак вірусів-вимагачів у порівнянні з традиційними підходами.

5. Вдосконалено метод симуляції кібератак за допомогою моделі емуляцій дій шахрая для тестування та оцінки ефективності розроблених моделей, одночасно, включаючи запуск вірусів-вимагачів у контрольованому лабораторному середовищі. Це дозволило детально аналізувати реакцію моделей на різноманітні сценарії атак та оптимізувати їх для максимальної ефективності.

6. Отримали подальший розвиток методики порівняльного аналізу та оцінки ефективності математичних апаратів виявлення та протидії програмам-вимагачам, за допомогою метрики MCC (коефіцієнту кореляції Метью), що виявився ефективнішим для оцінювання моделей, які працюють з незбалансованими даними, характерними для сценаріїв кіберзагроз типу вірусів-вимагачів.

Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна ґрунтується на професійному підході до формулювання дослідницьких завдань, коректному використанні аналітичного та числового апарату досліджень методів та логічно правильному обґрунтуванні прийнятих припущень при виборі математичних моделей.

Наукові положення дисертації є добре обґрунтованими та підтверджуються результатами експериментів, проведених автором. Використання сучасних методів машинного навчання та технології eBPF для виявлення програм-вимагачів є інноваційним підходом, що підтверджує новизну дослідження.

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

Наукові результати дисертації, що включають в себе розробку та інтеграцію модулів eBPF для моніторингу системних подій, файлової активності, мережевого трафіку та показників продуктивності, а також застосування моделей машинного навчання, таких як дерева рішень, метод опорних векторів та глибокі нейронні мережі, можуть бути використані для створення більш ефективних та адаптивних систем виявлення кіберзагроз. Ці результати можуть бути застосовані у різних наукових галузях, таких як інформаційна безпека, кібербезпека, машинне навчання та аналіз даних.

Розроблені методи та моделі можуть бути інтегровані у навчальні курси з кібербезпеки, машинного навчання та аналізу даних, надаючи студентам практичні навички та знання у сфері виявлення та протидії кіберзагрозам. Це особливо актуально для студентів спеціальностей, пов'язаних з інформаційними технологіями, комп'ютерними науками та інженерією.

Крім того, результати дослідження можуть бути використані для створення комерційних продуктів та послуг у сфері кібербезпеки, таких як програмне забезпечення для виявлення та протидії програмам-вимагачам, системи моніторингу та аналізу загроз, а також консалтингові послуги з кібербезпеки.

Також їх можна впровадити у навчальний процес у курсі " Інструменти мережевої безпеки та системи журналізації подій в Комп'ютерних системах" для студентів спеціальності 125 «Кібербезпека та захист інформації».

Практичне значення одержаних результатів полягає у тому, що:

Результати дослідження можуть бути корисними для фахівців з інформаційної безпеки, розробників антивірусного програмного забезпечення, а також для широкого кола користувачів комп'ютерних систем.

1. Використання розробленого комплексного методу аналізу даних на рівні ядра та ідентифікації програм-вимагачів із використанням фільтру eBPF, що значно підвищує швидкість та точність виявлення кіберзагроз. Впровадження

цього методу у системи кібербезпеки дозволяє оперативно відслідковувати та реагувати на підозрілі зміни в системних викликах, файловій активності та мережевому трафіку, сприяючи своєчасному виявленню атак.

2. Використання розробленої моделі класифікації на основі ансамблю дерев рішень та випадкового лісу продемонструвало підвищену точність у виявленні шкідливих програм, досягаючи в середньому точності вище 95% і F1-метрики 97.7%, що є значним внеском у розвиток інструментів кібербезпеки.

3. Застосування методології глибоких нейронних мереж для аналізу складних шаблонів даних демонструє передовий підхід до виявлення новітніх кіберзагроз. Розроблені моделі забезпечили точність ідентифікації на рівні 97.8%, прецизійність 96.9% та F1-метрику 97.7%, значно покращуючи аналітичні можливості комп'ютерних систем і забезпечуючи надійне виявлення невідомих раніше загроз та вірусів-вимагачів, що еволюціонують.

4. Проведені експерименти у контрольованому лабораторному середовищі підтвердили високу точність розроблених моделей, де модель на базі глибоких нейронних мереж продемонструвала точність до 97.8% і Коефіцієнт Кореляції Меттью (MCC) 0.95, що вказує на високий рівень адекватності та надійності виявлення кіберзагроз.

Основні результати дисертаційної роботи використано і впроваджено з метою покращення захищеності комп'ютерної мережі та систем в компанії ТОВ "ЕПАМ СИСТЕМЗ", реагування на інциденти кібербезпеки, компанією ТзОВ "ВІП СТУДІЯ" що підтверджено актами впровадження.

Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дисертаційної роботи Журавчака Даниїла Юрійовича викладено у пятнадцяти наукових публікаціях, а саме: семи статтях у наукових фахових виданнях України та восьми матеріалів конференцій, з яких три входить до міжнародної наукометричної бази Scopus.

Особистий внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей та результатів.

Зауваження по дисертації.

1. У розділі 3.3, присвяченому машинному навчанню, автор перераховує різні моделі та алгоритми, але не надає достатньо глибокого аналізу їх переваг та недоліків у контексті виявлення програм-вимагачів. Більш детальний розгляд допоміг би краще зрозуміти, чому були обрані саме ці моделі, і як вони взаємодіють з даними, отриманими від eBPF.

2. У розділі 2, присвяченому використанню eBPF, автор розглядає переваги цієї технології, такі як висока швидкість та гнучкість, але недостатньо уваги приділяє потенційному впливу eBPF на продуктивність системи. Більш детальний аналіз цього аспекту був би корисним для розуміння практичної застосовності запропонованих методів.

3. У розділі 1.7, де обговорюється вибір напряму дослідження, автор не приділяє достатньо уваги етичним аспектам використання технології eBPF та машинного навчання у контексті кібербезпеки. Враховуючи потенційні ризики для конфіденційності та безпеки даних, було б важливо розглянути ці питання більш детально.

4. У розділі 4, де представлено результати експериментів, автор не надає достатньо інформації про аналіз похибки вимірювань та статистичну значущість отриманих результатів. Це ускладнює оцінку надійності та відтворюваності результатів дослідження.

5. У розділі 1.5, де розглядаються SIEM та EDR рішення, автор не проводить порівняння цих систем з іншими засобами виявлення програм-вимагачів, такими як антивірусне програмне забезпечення або системи виявлення вторгнень. Це ускладнює розуміння місця запропонованого підходу в контексті існуючих рішень.

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

Висновок

Дисертаційна робота Журавчака Даниїла Юрійовича на тему "Удосконалення методів виявлення програм-вимагачів в режимі реального часу"

є завершеним та цілісним науковим дослідженням, що містить достатню наукову новизну та практичну цінність отриманих результатів. Дисертаційна робота заслуговує позитивної оцінки, відповідає вимогам наказу Міністерства освіти і науки України № 40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації», постанові Кабінету Міністрів України №44 від 12.01.2022 р. «Порядок присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії». а її автор, Журавчак Даниїл Юрійович заслуговує на присудження ступеня доктора філософії за спеціальністю 125 «Кібербезпека»

Офіційний рецензент
Кандидат технічних наук,
старший викладач кафедри захисту інформації Національного університету
“Львівська політехніка” Андрій ПАРТИКА

Підпис к.т.н, ст.викладача Партики А.І. засвідчую
Вчений секретар Роман БРИЛИНСЬКИЙ
Національного університету
“Львівська політехніка”
к.т.н., доцент