Облікова картка дисертації

I. Загальні відомості

Image not found or type unknow

Державний обліковий номер: 0824U002923

Особливі позначки: відкрита

Дата реєстрації: 29-08-2024

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Журавчак Даниїл Юрійович

2. Danyil Zhuravchak

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: 125 кібербезпека

Дата захисту: 13-08-2024

Спеціальність за освітою: кібербезпека

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ID 5936

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56, 20.56.01

Тема дисертації:

1. Удосконалення методів виявлення програм-вимагачів в режимі реального часу

2. Improvement of real time ransomware detection methods

Реферат/анотація:

1. В дисертаційній роботі вирішено важливу науково-практичну проблему з підвищення ефективності виявлення програм-вимагачів в інфраструктурі інформаційних систем шляхом використання моделей машинного навчання та технології eBPF. 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. Вперше запропоновано комплексну модель класифікації вірусіввимагачів 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. 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. 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. 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. 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.

2. The dissertation solved an important scientific and practical problem of increasing the effectiveness of detecting ransomware in the infrastructure of information systems by using machine learning models and eBPF technology. For the first time, a model of an integrated data collection system for the detection of ransomware viruses has been developed, combining the use of eBPF for monitoring system calls, file and cryptographic activity, network traffic and process analysis. This system provides a unique set of data (features) that are used to effectively identify potential threats in real time. For the first time, a complex model for classification of ransomware viruses using an ensemble of decision trees and a random forest is proposed, which allows to distinguish "safe" and "dangerous" programs with high accuracy based on the analysis of complex behavioral patterns and cryptographic activity. For the first time, a methodology for applying deep neural networks is proposed to identify complex patterns in data collected by eBPF modules representing the behavior of ransomware viruses, providing a new level of accuracy in detecting unknown or evolved threats. The methods of detecting cyber threats by analyzing network traffic using eBPF have been further developed, which significantly increases the speed and accuracy of identifying potential ransomware attacks compared to traditional approaches. The method of simulating cyberattacks with the help of a fraudster's action emulation model has been improved to test and evaluate the effectiveness of the developed models, simultaneously, including the launch of ransomware viruses in a controlled laboratory environment. This made it possible to analyze in detail the response of models to various attack scenarios and optimize them for maximum efficiency. Received further development: methods of comparative analysis and evaluation of the effectiveness of mathematical devices for detecting and countering ransomware programs, using the MCC metric (Matthew's correlation coefficient), which proved to be more effective for evaluating models that work with unbalanced data, typical of cyber threat scenarios such as ransomware viruses.

Державний реєстраційний номер ДіР: 0119U101690

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 1. Zhuravchak, D. "Створення системи запобігання поширення вірусів вимагачів за допомогою мови програмування Python та утиліти Auditd на базі операційної системи Linux". Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", вип. 4, вип. 12, Червень 2021, – С. 108-16.
- 2. Zhuravchak Danyil, Opanovych Maksym, Dudykevych Valerii, Piskozub Andrian. Detection Method Of Credential Dumping Method Through Exploiting Vulnerable Windows Error Reporting Service In Windows Operating Systems. Сучасна спеціальна техніка, – 2022. № 2 (69), С. 38-52.
- 3. Zhuravchak, D. ., V. Dudykevych, A. Tolkachova. "Дослідження структури системи виявлення та протидії атакам вірусів вимагачів на базі Endpoint detection and response". Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", вип. 3, вип. 19, Березень 2023, – С. 69-82.

- 4. Zhuravchak, D., Tolkachova, A., Piskozub, A., Dudykevych, V., Korshun, N. Monitoring ransomware with Berkeley packet filter // CEUR Workshop Proceedings, vol. 3550, Cybersecurity Providing in Information and Telecommunication Systems II 2023. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II co-located with the International Conference on Problems of Infocommunications. Science and Technology (PICST 2023), Kyiv, Ukraine, October 26, 2023 (online), 2023, pp. 95-106.
- 5. Піскозуб А.З., Журавчак Д.Ю., Толкачова А.Ю. Дослідження вразливостей у чатботах з використанням великих мовних моделей / Безпека Інформації, – 2023, № 3, том 29. С. 111-117.
- 6. Д.Журавчак, П.Глущенко, М.Опанович, В.Дудикевич, А.Піскозуб. Концепція нульової довіри для захисту active directory для виявлення програм-вимагачів // Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", вип. 2, вип. 22, Грудень 2023, с. 179-90.
- 7. Журавчак Даниїл, Едуард Кійко, Валерій Дудикевич. Використання EBPF для ідентифікації вірусів-вимагачів, що використовують DNS-запити DGA // Information Technology and Security, vol. 11, no. 2 (21), 2023, pp. 166-174.
- 8. Журавчак Д. Ю. Моніторинг вірусів-вимагачів за допомогою розширеного Берклійського пакетного фільтра (eBPF) та машинного навчання // Наукоємні технології, том 60, № 4, – 2023, С. 352-363.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Дудикевич Валерій Богданович

2. Valeriy B. Dudykevych

Кваліфікація: д.т.н., професор, 05.11.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович

2. Alexsey A. Smirnov

Кваліфікація: д.т.н., професор, 21.05.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, буд. 8, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Соколов Володимир Юрійович

2. Volodymyr Y. Sokolov

Кваліфікація: к. т. н., доцент, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Київський університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Партика Андрій Ігорович

2. Andriy I. Partyka

Кваліфікація: к. т. н., 05.27.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Совин Ярослав Романович
2. Sovyn Yaroslav R.

Кваліфікація: к. т. н., доц., 05.11.17

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Опірський Іван Романович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Опірський Іван Романович
Відповідальний за підготовку облікових документів	Пархуць Любомир Теодорович
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Тетяна Анатоліївна