Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0519U001709

Особливі позначки: відкрита

Дата реєстрації: 05-11-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Савенко Олег Станіславович
2. Savenko Oleg S.

Кваліфікація: к. т. н., 05.13.13

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 25-10-2019

Спеціальність за освітою: математика

Місце роботи здобувача: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, 11, м. Хмельницький, Хмельницький р-н., Хмельницька обл., 29016, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 35.052.08

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. С. Бандери, 12, м. Львів, Львівська обл., 79013, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, 11, м. Хмельницький, Хмельницький р-н., Хмельницька обл., 29016, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23, 50.39

Тема дисертації:

1. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах

2. The Theory and Practice of Creating Distributed Malware Detection Systems on Local Area Networks

Реферат/анотація:

1. Дисертація присвячена вирішенню актуальної науково-технічної проблеми розроблення теорії і практики створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп’ютерних мережах для покращення ефективності його виявлення. В роботі розроблено удосконалену модель архітектури розподіленої системи виявлення зловмисного програмного забезпечення в локальних комп’ютерних мережах та модель архітектури її типових компонентів на основі структур Кріпке, а також метод взаємодії компонентів розподіленої багаторівневої системи виявлення зловмисного програмного забезпечення для підтримки її цілісності та визначення порядку передачі знань між її компонентами. Розроблені алгебраїчні системи та алгебри з введеними операціями на множині ЗПЗ для створення поведінкових сигнатур ЗПЗ з метою їх формалізованого представлення в системах виявлення. Розроблено метод виявлення бот-мереж у локальних комп’ютерних мережах, суть якого полягає в здійсненні активного

моніторингу системних подій та узгодженій взаємодії компонентів розподіленої системи при прийнятті рішення. Розроблено метод виявлення файлового зловмисного програмного забезпечення в локальних комп'ютерних мережах, який полягає в поєднанні роботи програмних агентів, що здійснюють виявлення зловмисного програмного забезпечення в окремих комп'ютерних системах.

2. The dissertation is devoted to the solution of the actual scientific and technical problem of development of the theory and practice of creation of the distributed systems of detection of malware in local computer networks in order to increase its reliability of detection. Addressing this is important in all areas where LANs are being used extensively. In the work the advanced model of architecture of the distributed system of detection of malware in local computer networks is developed, based on complex consideration of the requirements of distribution, decentralization, multilevel and self-organization, and the model of architecture of its typical components on the basis of the Strengths components with representation of components which they may be in operation. It allowed to take into account the presence of software modules in different states and became the basis for determining the security status of the whole distributed system and its components. A method of interaction between components of a distributed multilevel malware detection system was developed on the basis of maintaining its integrity and determining the order of knowledge transfer between its components and using established analytical dependencies between the security levels of software modules and the security level of the whole distributed multilevel system. The method is the basis for the development of a linking piece of software that organizes the interaction of the components of a distributed multilevel malware detection system on local computer networks. Algebraic systems and algebras have been developed with the introduction of multiple malware operations, which became the basis for creating behavioral signatures of malware for their formalized representation in detection systems. The method of discovery of botnets in local computer networks was developed, the essence of which is to carry out active monitoring of system events and coordinated interaction of components of the distributed system when making a decision, made it possible to create tools that are able to integrate into the distributed system and to classify botnets for them behavioral signatures formed by the functions embedded in their components. The method of detecting malware on local computer networks has been developed, which consists in combining the work of software agents that detect malware in individual computer systems, according to the methods implemented in them: dynamic formation of behavioral signatures by tracking calls by example software interface, finding polymorphic and metamorphic program code, scanning executable programs by creating them autonomously these processes and related software agents in a distributed system. A method for detecting malware is based on the dynamic formation of behavioral signatures by tracking API-calls. It can be used to detect other types of virus programs, including new versions of existing viruses. The method involves the formation of a signature of a viral program based on the trace of API-calls, which allows to detect a viral program represented by a developed behavioral signature from the signature base. The behavioral signature includes critical API-calls by malicious activity groups and reflects the frequency of their occurrence, as well as the nature of the interaction of the critical API-features of the viral program and describes the relationship between the critical API-functions. This makes it possible to differentiate virus programs from useful applications not only in the presence of critical API challenges, but also in their interaction with each other. Classification is used to detect this. For the file-based API that uses entanglement techniques, a method for detecting polymorphic and metamorphic viruses has been developed based on an analysis of obfuscation functions. The peculiarity of the method is the analysis of the software object and its modified versions, obtained from different modules, and further analysis based on the search for equivalent functional blocks. This allows a more detailed analysis of the software object code for the presence of polymorphic and metamorphic viruses.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Саченко Анатолій Олексійович
2. Sachenko Anatoliy O.

Кваліфікація: д. т. н., 05.11.16

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Саченко Анатолій Олексійович
2. Sachenko Anatoliy O.

Кваліфікація: д. т. н., 05.11.16

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Дрозд Олександр Валентинович
2. Drozd Oleksandr V.

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Мухін Вадим Євгенійович
2. Mukhin Vadym

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Мельник Анатолій Олексійович
2. Melnyk Anatoliy Oleksiyovych

Кваліфікація: д.т.н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Стадник Богдан Іванович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Стадник Богдан Іванович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.