DOI 10.31891/2307-5732-2024-331-2
УДК 004.75:004.49:004.52

САВЕНКО БОГДАН
Хмельницький національний університет
https://orcid.org/0000-0001-5647-9979
e-mail: savenko_bohdan@ukr.net

МЕТОД ВИЯВЛЕННЯ WORM-ВІРУСІВ ЗГІДНО БАГАТОКЛАСОВОЇ КЛАСИФІКАЦІЇ

В роботі наведено результати досліджень щодо worm-вірусів і методів їх виявлення. Розповсюдження зловмисного програмного забезпечення відбувається постійно. Проаналізовані сучасні засоби та системи попередження, виявлення та протидії зловмисному програмному забезпеченню і комп'ютерним атакам є досить ефективними, забезпечують великий відсоток виявлення та функціонують на належному рівні. Але зловмисники постійно вивчають спроможності таких засобів та систем, вдосконалюють зловмисне прогармне забезпечення та здійснення комп'ютерних атак і досягають певних результатів. Тому, розробники засобів та систем попередження, виявлення та протидії зловмисному програмному забезпеченню і комп'ютерним атакам повинні постійно їх вдосконалювати. Актуальним є захист корпоративних мереж. Вони можуть бути ефективно конфігуровані для збільшення обчислювальних ресурсів при вирішенні завдань попередження, виявлення та протидії зловмисному програмному забезпеченню і комп'ютерним атакам для захисту корпоративних мереж.Тому, в статті визначено як актуальну наукову задачу - розроблення методів для покращення ефективності функціонування розподілених систем з частковою централізацією для виявлення зловмисному програмному забезпеченню і комп'ютерним атакам в комп'ютерних мережах та виявлення зловмисного програмнонр забезпечення з їх використанням за рахунок синтезу їх архітектури таким чином, щоб принципи функціонування таких систем ускладнювали зловмисниками їх розуміння.

В роботі розглядається множина worm-вірусів, яка максимально охоплює мережні особливості. Тому, для дослідження ефективності методів створення розподілених систем і на їх основі самих систем було розглянуто worm-віруси.

Метою роботи є розроблення методу виявлення worm-вірусів в корпоративних мережах.

В роботі розроблено метод виявлення worm-вірусів з використанням поділу їх на класи за спільними ознаками і визначеними критеріями згідно класифікації об'єктів за багатьма класами і з врахуванням імплементації його в архітектуру частково централізованих розподілених систем для отримання цілісного сенсору та прийнятті рішення щодо віднесення worm-вірусу до певного класу. Це покращило достовірність виявлення на 8-11% порівняно з використанням методу без залучення безпосередньо елементів та компонентів системи. В результаті здійснення постановки експериментів та їх проведення було отримано результати, які підтверджують коректне функціонування частково централізованої розподіленої системи до виявлення worm-вірусів.

Ключові слова: розподілені системи, комп'ютерні мережі, часткова централізація, зловмисне програмне забезпечення, worm-вірус.

SAVENKO BOHDAN
Khmelnytskyi National University

WORM-VIRUS DETECTION METHOD ACCORDING TO MULTI-CLASS CLASSIFICATION

The work presents the results of research on worm viruses and methods of their detection. Malware distribution happens all the time. The analyzed modern tools and systems for prevention, detection and countermeasures against malicious software and computer attacks are quite effective, provide a high percentage of detection and function at an adequate level. But criminals constantly study the capabilities of such tools and systems, improve malicious software and computer attacks, and achieve certain results. Therefore, developers of tools and systems for prevention, detection and countermeasures against malicious software and computer attacks must constantly improve them. The protection of corporate networks is relevant. They can be effectively configured to increase computing resources when solving the tasks of warning, detecting and countering malicious software and computer attacks to protect corporate networks. Therefore, the article defines as an urgent scientific task - the development of methods to improve the efficiency of the functioning of distributed systems with partial centralization for detection of malicious software and computer attacks in computer networks and detection of malicious software with their use due to the synthesis of their architecture in such a way that the principles of functioning of such systems make it difficult for criminals to understand them.

The work considers a set of worm viruses, which covers network features as much as possible. Therefore, to study the effectiveness of methods of creating distributed systems and the systems themselves based on them, worm viruses were considered.

The purpose of the work is to develop a method for detecting worm viruses in corporate networks.

The work developed a method of detecting worm viruses using their division into classes based on common features and defined criteria according to the classification of objects according to many classes and taking into account its implementation in the architecture of partially centralized distributed systems to obtain a complete sensor and make a decision regarding the classification of worms virus to a certain class. This improved the reliability of detection by 8-11% compared to using the method without directly involving the elements and components of the system. As a result of setting up experiments and conducting them, results were obtained that confirm the correct functioning of a partially centralized distributed system for the detection of worm viruses.

Keywords: distributed systems, computer networks, partial centralization, malicious software, worm virus.

Постановка проблеми

Розповсюдження зловмисного програмного забезпечення (ЗПЗ) відбувається постійно та постійно зростає [1-3]. Сучасні засоби та системи попередження, виявлення та протидії ЗПЗ і комп'ютерним атакам (КА) є досить ефективними, забезпечують великий відсоток виявлення та функціонують на належному рівні. Але зловмисники постійно вивчають спроможності таких засобів та систем, вдосконалюють ЗПЗ та здійснення КА і досягають певних результатів. Тому, розробники засобів та систем попередження, виявлення

та протидії ЗПЗ та КА повинні постійно їх вдосконалювати. Особливо актуальним є захист корпоративних мереж, які в сукупності є типовим класом об'єктів, до якого можуть бути застосовані ефективні типові рішення. Цей клас об'єктів порівняно з одиничними комп'ютерними станціями може бути ефективно конфігурований для збільшення обчислювальних ресурсів при вирішенні завдань попередження, виявлення та протидії ЗПЗ та КА для захисту корпоративних мереж.

Крім нових чи удосконалення відомих методів попередження, виявлення та протидії ЗПЗ та КА, важливим та перспективним напрямом залишається напрям з дослідження, удосконалення чи створення принципово нової архітектури [4] засобів та систем попередження, виявлення та протидії ЗПЗ та КА їх розробниками. Така архітектура повинна включати можливості систем до інтеграції в неї методів виявлення і результатом такого поєднання повинен виступати цілісний сенсор, в якому буде наявний центр для прийняття рішень, методи виявлення та підсистема залучення обчислювальних ресурсів комп'ютерних станцій, з яких сформовано систему. Також, така архітектура повинна бути основою для розроблення систем, які будуть важко зрозумілими для зловмисників та важко прогнозованими її дії. Оскільки, зловмисники можуть бути присутніми і в межах периметру захисту корпоративної мережі. В цьому контексті важливою вимогою до системи є її спроможність приймати рішення без втручання користувача. Все це в сукупності вимагає синтезувати в архітектурі таких систем ефективний центр прийняття рішень, який міг би, також, переміщуватись в залежності від зміни стану в корпоративній мережі та безпосередньо в системі.

Дослідження та розроблення архітектури розподілених систем попередження, виявлення та протидії ЗПЗ та КА саме з спрямуванням на особливості та варіанти їх центру прийняття рішень, а також дослідження, відповідно, впливу на ефективність та достовірність таких систем, є недостатнім. Крім того, не тільки безпосередньо центр прийняття рішень як цілісна частина системи впливатиме на її функціонування, а саме його архітектура та принцип реалізації є перспективним напрямом для дослідження. Найбільш дослідженими є системи з централізованою та децентралізованою архітектурою в контексті завдань з попередження, виявлення та протидії ЗПЗ та КА. Але недостатньо досліджена архітектура розподілених систем з частковою централізацією. Вона актуальна для систем з приховуванням їх особливостей та розуміння їх функціонування зловмисниками.

Тому, актуальною науковою задачею є розроблення методів для покращення ефективності функціонування розподілених систем з частковою централізацією для виявлення ЗПЗ та КА в комп'ютерних мережах та виявлення ЗПЗ з їх використанням за рахунок синтезу їх архітектури таким чином, щоб принципи функціонування таких систем ускладнювали зловмисниками їх розуміння.

Аналіз останніх досліджень і публікацій

Розподілені системи попередження, виявлення та протидії ЗПЗ функціонують в корпоративних мережах. Тому, розглянемо їх спрямування щодо попередження, виявлення, запобігання, протидії та реагування до мережного типу ЗПЗ. Хоча розподілені системи можуть здійснювати виявлення ЗПЗ, також, в окремих комп'ютерних станціях. До мережного ЗПЗ відноситься багато різноманітних типів за різними критеріями поділу. Але найбільш широко позиціонованим є множина worm-вірусів. Вони поширюються комп'ютерними мережами, часто стають основою розбудови бот-мереж [5-7], можуть бути цілеспрямованим, можуть переносити частини іншого ЗПЗ, принципово відрізняються за будовою від багатьох класів комп'ютерних вірусів, які спрямовані на інфікування виконуваних PE-файлів. Тому, розглядатимемо множину worm-вірусів як об'єкти для дослідження розподіленими системи, оскільки переважна більшість процесів для розподілених систем та worm-вірусів буде відбуватись саме в комп'ютерних мережах. Синтез розподілених систем потрібно здійснювати так [4, 8, 9], щоб в їх архітектуру можна було імплементувати не одиничні методи попередження, виявлення, запобігання, протидії та реагування на дії ЗПЗ, а багато різних і для різних типів ЗПЗ та КА. Може бути так, що для одного класу певного типу ЗПЗ потрібно декілька методів. ЗПЗ може бути таким, що тривалий час приховує свою присутність і розподілена система повинна вміти протидіяти і таким загрозам. Наприклад [10], в США було виявлено ЗПЗ, яке надавало таємний доступ до комп'ютерів жертв, дозволяючи пристроям, в яких воно функціонувало, таємно спілкуватися один з одним і діючи як плацдарм для додаткової зловмисної активності. Тому, системи повинні бути комплексними і їх архітектура, відповідно, повинна враховувати потреби в її наповнені багатьма методами. Це підтверджено фахівцями, наприклад в [11, 12]. Зокрема, в [11] акцент зроблено на комплексні рішення для управління безпекою за допомогою комплексних можливостей запобігання, виявлення та реагування згідно штучного інтелекту, провідних досліджень загроз і розвідки. А система Zeek (Bro) [12], яка є платформою для аналізу трафіку, орієнтована пріоритетно на відстеження подій, пов'язаних з безпекою, не обмежується тільки цим застосуванням. В ній наявні модулі для аналізу і опрацювання різних мережних протоколів програм, що враховують стан з'єднань і дозволяють формувати детальний журнал (архів) мережної активності.

Розглянемо worm-віруси [13] в контексті їх особливостей, застосування та будови. В роботах [14, 15] представлено декомпозицію вірусів і worm-програм згідно їх основних функційних компонентів. В роботі [16] здійснено аналіз окремої ЗПЗ «троянський кінь», який під час виконання може змінювати інші комп'ютерні програми, наприклад, копіюючи себе (або частину) у них. В роботі [17] зловмисні програми аналізуються на наявність ознак вірусів, worm-вірусів, троянських програм і руткітів та пропонуються конкретні контрзаходи, для їх розпізнавання. У роботі [18] побудовано модель SIQR розповсюдження worm-вірусу залежно від двофакторної моделі. У роботі [19] зроблено припущення про існування багатовекторних worm-вірусів. В ній подано пару з них за слідами нападу, які зібрані в приманці. У роботі [20] проаналізовано приклади ЗПЗ:

віруси, worm-віруси, троянські програми, шпигунське програмне забезпечення, клавіатурні шпигуни, ботнети, руткіти, програмне забезпечення для вимагання та випадкові завантаження. Розробники ЗПЗ стають професійнішими в здатності розробляти ефективне ЗПЗ, яке складно виявляти [10, 20-22], і тому розробникам систем протидії ЗПЗ потрібно постійно залишатися інноваційними, щоб вдосконалювати методи та системи протидії ЗПЗ. Підтвердження нестандартних рішень, наприклад, щодо троянських програм подано в роботі [23, 24]. Апаратні трояни вважаються одним з найнебезпечніших видів зловмисного порушення цілісності систем на основі FPGA. Дослідження довело, що апаратні трояни можуть бути імплантовані в систему (або проект системи) під час її планової модифікації. Зокрема, це відбувається, коли не працює моніторинг цілісності, базований на використанні хеш-суми. Перед запуском моніторингу цілісності слід переконатися, що апаратні трояни не імплантовані. Автори запропонували метод виявлення розташування апаратних троянів у просторі компонентів на основі FPGA критичних для безпеки систем. Дослідження троянських програм в роботі [25] підтверджує використання стандартних засобів для забезпечення спілкування між скомпрометованими вузлами за різними моделями зловмисників [25, 26]. Worm-віруси можуть бути застосовні у взаємодії із троянськими програмами, а також для побудови бот-мереж. В роботі [27] розглянуто різні моделі бот-мереж та запропоновано рішення, яке сформоване з використанням мультиагентної системи, для дослідження зловмисної активності в мережах.

Для забезпечення ефективного результату з виявлення ЗПЗ та КА потрібно, крім методів виявлення, також і ефективні системи. В роботі [28] подано комплексне рішення щодо перспектив забезпечення кібербезпеки, яке включає також і погляд на систему, яка потребує захисту, та побудову системи захисту. В роботі [29] пропонується використовувати приманки для виявлення ЗПЗ і приділено увагу системі, в якій вони реалізовані. Така система є розподіленою [4, 29]. В роботі [30] подано еволюційну мережну модель тестування розподілених систем, яка може бути використана для проєктування таких систем. Перспективність такого напряму досліджень і розвитку підтвердується, також, в [31, 32]. Системи запобігання вторгненням для бездротових мереж (WIPS) [31] відстежують активність у бездротових мережах. А системи аналізу поведінки мережі (NBA) [32] аналізують мережевий трафік для виявлення незвичайних моделей. Аналіз поведінки мережі визначається як процес збору та аналізу корпоративних мережевих даних для виявлення незвичної поведінки об'єктів, яка може свідчити про зловмисну діяльність. Взагалі існує дві основні стратегії в сфері виявлення атак: виявлення зловживань (misuse detection) і виявлення аномалій (anomaly detection). Але в обох випадках для корпоративних мереж основою їх реалізації є розподілені системи. Методи розподіленого управління корпоративними комп'ютерними мережам подано в [33]. Вимоги до розподілених обчислень задані в стандарті [34]. Методи ідентифікації аномальних станів для систем виявлення вторгнень подано в роботі [35]. Методи виявлення зловживань, зокрема з використанням ЗПЗ та КА, подано в роботах [36-38].

Для розподілених систем важливо забезпечити їх стійкість, особливо в умовах впливу КА та ЗПЗ безпосередньо на них. Методологічні основи та інформаційна технологія забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз подана в роботах [39, 40]. Методи забезпечення відмовостійкості та живучості розподілених систем в умовах впливів зловмисного програмного забезпечення подано в роботі [41]. Процеси кіберзахисту [42] відносяться до випадкових багатовимірних, динамічних нестаціонарних, активних (цілеспрямованих), що ускладнює завдання прогнозування показників кіберзахищенності. В роботі [42] запропоновано алгоритм вибору показників прогнозування кіберзахищенності комп'ютерних систем. У роботі [43] пропонується стратегія для оцінки надійності, доступності та кібербезпеки хмари та системи Інтернету речей на основі безперервного збору, порівняння, вибору та поєднання марковських і напівмарковських моделей. Отриманими результатами були алгоритми для збору та аналізу даних, вибору та поєднання відповідних моделей та їх різних типів, таких як багатофрагментні та багатофазові моделі, враховуючи зміну рівня відмов, параметрів кібератак, періодичного обслуговування тощо. Методологічні основи забезпечення функціональної стійкості розподілених систем до кібернетичних загроз подано в роботі [44]. Таким чином, розроблення розподілених систем потрібно здійснювати з врахуванням забезпечення їх стійкості не тільки через забезпечення функційної безпеки, але й в умовах впливу КА та ЗПЗ безпосередньо на них.

Worm-вірус характеризується тим, що це тип ЗПЗ, який має визначальну мету, що полягає в поширенні його на велику кількість комп'ютерів з використанням мереж. В українській антивірусній компанії «Zillya Антивірус» [45] для worm-вірусів виділено такі методи розмноження: через вразливості програмного забезпечення; за допомогою програм для спілкування; через мережні ресурси; через P2P мережі каналами файлообмінних пірінгових мереж. Засоби, які при цьому використовуються worm-вірусами, що закладені в них зловмисниками, та функції повинні бути предметом аналізу для їх виявлення [46]. Наприклад [47], "Хробак Моріса" намагався підібрати паролі до облікових записів. Для цього використовував ім'я користувача і список із 400 найбільш популярних слів. "Хробак" використовував маскування, щоб приховати свою присутність у комп'ютері. Він видаляв свій виконуваний файл, перейменовував свій процес у sh [47]. Тому, розробники систем протидії ЗПЗ повинні включати в них аналіз функцій, що забезпечують мережну комунікацію, та їх комбінацій [48].

Згідно аналізу наукових результатів [6, 13-22] встановлено різноманітність worm-вірусів, яка проявляється не тільки за основним типом розповсюдження, але й за використанням з різними іншими комп'ютерними вірусами та троянськими програмами, а також, можлива наявність у worm-вірусів багатовекторності.

Таким чином, універсальні підходи та стратегії до створення розподілених систем виявлення ЗПЗ не можуть бути застосовані, зокрема і для мережного ЗПЗ. Оскільки зловмисники після ознайомлення з ними можуть зрозуміти як працюють такі системи і використати це для здійснення КА та в ЗПЗ. Тобто, створити декілька стандартних розподілених систем універсального призначення з різною архітектурою і наповнювати їх різними функціями (методами), зокрема і тими, які виявляють, протидіють ЗПЗ, не доцільно. Тому, для розподілених систем саме такого призначення потрібно синтезувати особливий набір характеристик в їх архітектурі і цим вони будуть відрізнятись від універсальних розподілених систем. Важливою характеристикою розподілених систем такого призначення є їх стійкість до впливів ЗПЗ та КА і, тому цей напрям при створенні розподілених систем потрібно враховувати. Як для вирішення завдань попередження, виявлення та протидії ЗПЗ і КА так і для забезпечення стійкості функціонування розподілених систем потрібно сформувати набір показників [48] в корпоративній мережі, які б система могла аналізувати для подальшого прийняття рішень.

Зловмисники продовжують створювати ефективне ЗПЗ і такі дії мають стійку тенденцію до зростання, як кількісно, так і за охопленням різних типів. Для корпоративних мереж використовуються відомі засоби, але вони не забезпечують повного виявлення та надійної протидії ЗПЗ. Це підтверджується відповідними результатами незалежних антивірусних лабораторій та самими розробниками. Тому, є потреба в подальшій розробці нових систем та методів для попередження, виявлення та протидії ЗПЗ в корпоративних мережах, які повинні бути розподіленими. Розроблені, таким чином, розподілені системи могли б бути наповнені різними методами попередження, виявлення та протидії ЗПЗ і КА та, при цьому, могли б мати різне призначення. Вони могли б бути системами попередження, або системами виявлення, комплексними системами, системами з приманками тощо.

Оскільки розроблення методів стосується створення розподілених систем, які будуть функціонувати в корпоративних мережах, то для врахування особливостей ЗПЗ, якому вони будуть протидіяти проаналізовано мережне ЗПЗ, зокрема worm-віруси. Зловмисники при їх реалізації використовують стандартний набір доступних функцій та засобів співвіднесено до середовища їх функціонування, зокрема корпоративних мереж та їх особливостей. Тому, саме множина worm-вірусів максимально охоплює мережні особливості. Решта типів ЗПЗ теж може мати при створенні такі або частину функцій та засобів як і worm-віруси. Але в них буде інше спрямування і це зменшуватиме для всієї їх множини відсоток застосування таких функцій і засобів порівняно з worm-вірусами. Тому, для дослідження ефективності методів створення розподілених систем і на їх основі самих систем будемо розглядати worm-віруси.

Метою роботи є розроблення методу виявлення worm-вірусів в корпоративних мережах.

Виклад основного матеріалу

В комп'ютерних мережах може перебувати різноманітне ЗПЗ. Завдяки технологіям та засобам підтримки функціонування комп'ютерних мереж, крім корисного їх застосування, наявні широкі можливості їх використання зловмисниками. Наприклад, для створення бот-мереж зловмисники можуть використовувати стандартні засоби роботи з пересилання повідомлень та файлів, команди, а також можуть для досягнення своєї мети, щоб приховати свої зловмисні дії, використати мережні віруси для проникнення у вузли в мережах та встановлення в них контролю. Такими вірусами можуть бути worm-віруси. Розглянемо їх в контексті їх цілеспрямованого поширення і отримання контролю завдяки їм над комп'ютерними станціями в корпоративних мережах, а не випадкового поширення з метою нанесення шкоди користувачам комп'ютерів, які під'єднані до глобальної мережі. Шкода від таких вірусів може обмежуватись зниженням пропускної здатності. Worm-віруси на відміну від звичайних комп'ютерних вірусів, мають певні особливості. Визначальною особливістю є спрямування worm-вірусів на інфікування переважно комп'ютерів, а не файлів в них, і цільова функція спрямована саме на досягнення максимізації інфікування кількості комп'ютерів, а не файлів в них. Хоча можуть бути і такі, що додатково спрямовані на інфікування файлів в комп'ютерних станціях, в які отримали доступ. Маючи такий функціонал у worm-вірусах щодо їх поширення і спрямування саме для поширення в комп'ютерних мережах, як локальних так і глобальних, зловмисники можуть їх використати для цілеспрямованого охоплення корпоративної мережі, яка їх цікавить та, як наслідок, навколо якої можуть створити зони поширення таких worm-вірусів. Тому, захищаючи корпоративну мережу частково централізованими системами потрібно імплементувати в них підсистеми та засоби протидії такому зловмисному програмному забезпеченню, як worm-віруси. Введемо множину W worm-вірусів так:

$$W = \{w_1, w_2, \dots, w_{N_w}\}, \quad (1)$$

де w_i - i - worm-вірус; N_w – кількість відомих worm-вірусів.

Для виявлення worm-вірусів здійснимо аналіз їх будови, типів розмноження та поширення. Це дасть змогу виділити типові характеристики. За поєднанням типових характеристик здійснимо поділ елементів множини W на класи. Цей поділ дасть змогу виділити особливі характеристики у worm-вірусів певних класів, що покращить ефективність їх виявлення та дасть змогу чіткіше відокремити їх від корисних програм чи процесів. Задамо характеристичні показники worm-вірусів множиною $M_W = \{m_{W,1}, m_{W,2}, \dots, m_{W,N_W}\}$, де N_W – кількість характеристичних показників, $m_{W,i}$ - i-ий характеристичний показник, $i = 1,2, \dots, N_W$. Деталізуємо кожен характеристичний показник з метою подальшого поєднання їх елементів для задання відповідно типу worm-вірусів.

Розглянемо перший характеристичний показник, який характеризує тип розмноження, тоді елемент $m_{W,1}$ – характеристичний показник типів розмноження worm-вірусів. Деталізуємо його так: $m_{W,1,1}$ - розмноження worm-вірусів, яке забезпечується за рахунок вразливостей програмного забезпечення; $m_{W,1,2}$ – розмноження worm-вірусів, яке забезпечується за допомогою програм для спілкування; $m_{W,1,3}$ – розмноження worm-вірусів, яке забезпечується за допомогою електронної пошти та адрес; $m_{W,1,4}$ – розмноження worm-вірусів, яке забезпечується за допомогою мережних ресурсів; $m_{W,1,5}$ – розмноження worm-вірусів, яке забезпечується за допомогою P2P мережі каналами файлообмінних пірінгових мереж. Елемент $m_{W,1,3}$ може бути поділений на два такі випадки: $m_{W,1,3,1}$ характеризує масову розсилку на всі електронні пошти; $m_{W,1,3,2}$ характеризує розсилку на визначені адреси електронної пошти. Конструктивно worm-віруси можуть поєднувати декілька $m_{W,1,j}$ $(j = 1,2,\dots,5)$, формуючи таким чином багатовекторність. Завдяки наявності декількох механізмів розмноження зростають можливості його поширення в комп'ютерних мережах.

Worm-вірус надходить в комп'ютерну станцію мережею в форматі виконуваного файлу і активізується в ній після його запуску. Тому, другим важливим характеристичним показником $m_{W,2}$ є структура worm-вірусів. Виділимо різні за призначенням елементи типових структур так: $m_{W,2,1}$ – експлойт (або двійковий виконуваний код) і розміщене в оперативному запам'ятовуючому пристрої корисне навантаження; $m_{W,2,2}$ - локальна частина корисного навантаження в оперативній пам'яті та завантаження решти worm-вірусу окремим файлом засобами комп'ютерної мережі; $m_{W,2,3}$ - один файл; $m_{W,2,4}$ – решта варіантів. Елемент $\mathrm{m_{W,2,1}}$ характеризує резидентні worm-віруси. Крім того, цей елемент може бути деталізований за ознакою відношення експлойта до певних об'єктів в комп'ютерних станціях так: $\mathrm{m_{W,2,1,1}}$ – використання для прикладного програмного забезпечення; $\mathrm{m_{W,2,1,2}}$ - використання для операційних систем; $\mathrm{m_{W,2,1,3}}$ - використання для браузерів; $\mathrm{m_{W,2,1,4}}$ – використання для сайтів; $\mathrm{m_{W,2,1,5}}$ – використання для спеціалізованого програмного забезпечення; $\mathrm{m_{W,2,1,6}}$ – використання для решти засобів, які використовуються в комп'ютерній станції та мають вразливості. Елемент $\mathrm{m_{W,2,3}}$ характеризує поштові worm-віруси.

При виборі за характеристичний показник елементу $m_{W,1}$ можна поділити всю множину worm-вірусів на такі класи: клас, в якому не міститься жодного елементу з характеристичним показником $m_{W,1,j}$ $(j = 1,2,\dots,5)$, тобто клас, в якому відсутні worm-віруси, і позначимо його K_W^0; клас K_W^j $(j = 1,2,\dots,5)$, який визначатиметься характеристичним показником $m_{W,1,j}$ $(j = 1,2,\dots,5)$, і всього таких класів буде п'ять; клас K_W^6, в який будуть віднесені елементи, для характеристики яких буде більше одного характеристичного показника $m_{W,1,j}$ $(j = 1,2,\dots,5)$. Побудова класу K_W^6 може бути здійснена системою S в процесі її функціонування при виявленні багатовекторних worm-вірусів. Для віднесення об'єкту до класу K_W^6 система S повинна встановити його мінімум в двох класах з класів K_W^j $(j = 1,2,\dots,5)$. Формування класу K_W^0 можливе за умови помилкового віднесення worm-вірусів до нього при застосуванні систем виявлення. При правильно здійсненій класифікації worm-вірусів клас K_W^0 буде порожнім, тобто $K_W^0 = \varnothing$. Наявність елементів в класі K_W^0 буде означати помилковість спрацювання відповідного детектора та системи в цілому. Таким чином, всю множину worm-вірусів поділимо на шість класів:

$$W = \bigcup_{j=1}^{6} K_W^j. \quad (2)$$

Отриманий поділ множини worm-вірусів на шість класів дає змогу здійснити фіксування характерних властивостей і може бути деталізований за певними визначеними критеріями.

Метод виявлення worm-вірусів згідно багатокласової класифікації за типовими характеристиками враховує поділ на класи та їх ознакове поле, яке включає поведінкові сигнатури worm-вірусів, аналітичні вирази характеристик згідно поведінкових сигнатур, шаблони атак та відбитки, які можуть бути отримані з приманок для worm-вірусів, а також зміни в оточуючому середовищі, тобто в корпоративній мережі. Метод імплементовано в архітектуру частково централізованої розподіленої системи. Тому, він передбачає опрацювання, також, стану функційної та кібербезпеки в корпоративній мережі.

Суть методу:

1) отримання інформації з сенсору щодо успішної / неуспішної спроби ззовні завантажити файл в оперативний запам'ятовуючий пристрій та створення і запуск процесу;

2) збір інформації щодо функціонування процесу з п. 1);

3) оновлення інформації щодо поточного стану частково централізованої розподіленої системи;

4) формування сигнатури процесу;

5) формування вектору для виконуваних в процесі функцій-підмножин;

6) формування шаблону атаки, якщо вона відбувається;

7) аналіз вмісту приманок та формування відбитку-шаблону, як результату;

8) пакету відомостей про процес в компєютерній станції в корпоративній мережі;

9) виконання кроку 7 (оцінювання результатів розподілених обчислень в компонентах) методу організації функціонування частково централізованих розподілених систем;

10) виконання кроку 8 (визначення компонент, в яких буде виконуватись поставлене системою завдання) методу організації функціонування частково централізованих розподілених систем;

11) класифікація процесу до класів worm-вірусів або до класу підозрілих процесів;

12) виконання кроку 9 (перебудова архітектури системи за наявності критичних подій) методу організації функціонування частково централізованих розподілених систем.

Розроблено метод виявлення worm-вірусів з використанням поділу їх на класи за спільними ознаками і визначеними критеріями згідно класифікації об'єктів за багатьма класами і з врахуванням імплементації його в архітектуру частково централізованих розподілених систем.

Результати експериментальних досліджень

При проведенні експериментів з системою S щодо достовірності виявлення зловмисного програмного забезпечення розглядатимемо як об'єкти дослідження worm-віруси [48]. Для проведення експериментальних досліджень спочатку здійснимо конструювання п'яти класів worm-вірусів по чотири екземпляри. Для цього використаємо конструктивні елементи формування штучних worm-вірусів без зловмисного навантаження та з корисним функціоналом, який повідомлятиме на екран про позитивний результат інфікування комп'ютерної станції і продовження розмноження в комп'ютерній мережі. При цьому на екран, також, буде видаватись інформація про час завершення повної процедури інфікування комп'ютерної станції. В усіх комп'ютерних станціях встановлено ОС Windows і всі комп'ютерні станції мають однакове конфігурування. Кількість комп'ютерних станцій, в які встановлено компоненти системи S, дорівнює сто, а кількість комп'ютерних станцій, в яких не встановлено компоненти системи S, дорівнює десять. Кількість сегментів, на які поділено корпоративну мережу, дорівнює п'ять. Корпоративна мережа містить два сервери.

Проведення експериментів з частково розподіленою системою S для перевірки достовірності виявлення worm-вірусів імплементованим в неї методом здійснимо з врахуванням шести типів джерел їх поширення [48]. Ці джерела будемо розглядати в контексті шістьох можливих варіантів. Під час проведення експериментів корпоративна мережа та додаткові десять комп'ютерних станцій, які не належать їй, будуть від'єднані від мережі Internet. Але ці десять комп'ютерних станцій будуть під'єднані до корпоративної мережі, як частина вузлів глобальної мережі.

При встановленні результатів експерименту [48] будемо розглядати чотири варіанти подій, які відбулись, і розподілимо їх так: тип worm-вірусу встановлено правильно і, відповідно, його віднесено до одного з класів K_W^j ($j = 1,2,\dots,5$), для якого проводились дослідження; заповнено клас $K_W^{0,j}$ ($j = 1,2,\dots,5$), тобто був пропущений worm-вірус в комп'ютерних станціях системою S, але відповідний штучний worm-вірус проінформував своїм корисним функціоналом про успішне інфікування комп'ютерної станції; система S віднесла до відповідного класу worm-вірусу об'єкт, який таким не був та, відповідно, не проінформував своїм корисним функціоналом про успішне інфікування комп'ютерної станції, і, тоді, виділимо його додатковим класом $K_W^{j,p}$ ($j = 1,2,\dots,5$); інфікування комп'ютерної станції не відбулось і компонент та система S це підтвердили та позначимо клас для цього варіанту як $K_W^{j,Y}$ ($j = 1,2,\dots,5$). Результати експериментів [48] задано в табл. 1.

Таблиця 1

Результати експерименту

Результат виявлення	Класи worm-вірусів, $j = 1,2,\dots,5$	Серії експерименту												Разом	Відсотки
		Екземпляри класу													
		1			2			3			4				
		1	2	3	4	5	6	7	8	9	10	11	12		
FN	$K_W^{0,j}$	344	320	302	376	345	267	307	298	267	348	317	393	3884	10,7889
TP	K_W^{j}	911	915	837	897	853	934	892	946	932	976	831	864	10788	29,9666
FP	$K_W^{j,p}$	184	198	129	115	124	160	214	253	94	172	208	84	1935	5,375
TN	$K_W^{j,Y}$	1561	1567	1732	1612	1678	1639	1587	1503	1707	1504	1644	1659	19393	53,8695

Здійснимо аналіз результатів експерименту.

Частку істинно позитивних випадків TPR (*True Positives Rate*) обчислюємо так:

$$TPR = \frac{TP}{TP+FN} \cdot 100\% = \frac{10788}{14672} \cdot 100\% = 73{,}5278\%. \quad (3)$$

Частку хибно позитивних випадків (False Positives Rate)

$$FPR = \frac{FP}{TN+FP} \cdot 100\% = \frac{1935}{21328} \cdot 100\% = 9{,}0726\%. \quad (4)$$

Для оцінювання достовірності виявлення worm-вірусів системою S та імплементованим в неї методом, як цілісного бінарного класифікатора, визначимо чутливість та специфічність моделі та обчислимо їх значення. Значення чутливості:

$$S_e = TPR = 73{,}5278\%. \quad (5)$$

Значення специфічності визначаємо як частку істино негативних випадків, які були правильно ідентифіковані, та обчислюємо так:

$$S_p = \frac{TN}{TN+FP} \cdot 100\% = \frac{19393}{21328} \cdot 100\% = 90{,}9274. \quad (6)$$

Оскільки значення специфічності є високим, то система S виявляє негативні випадки краще, ніж позитивні, бо чутливість є меншою порівняно з специфічністю.

Обчислимо, також, F1-міру. Вона характеризує класифікатор щодо виявлення позитивних екземплярів. Алгоритм знаходження F1-міри полягає в обчисленні середнього гармонічного між точністю (precision) та повнотою (recall) класифікаційної моделі. F1=0.5029 для результатів проведеного експерименту, що є достатнім, але потребуватиме подальше покращення методу виявлення worm-вірусів для досягнення збільшення цього значення.

Таким чином, в результаті здійснення постановки експериментів та їх проведення було отримано результати, які підтверджують коректне функціонування частково централізованої розподіленої системи до виявлення worm-вірусів.

Висновки

Таким чином, розроблено метод виявлення worm-вірусів з використанням поділу їх на класи за спільними ознаками і визначеними критеріями згідно класифікації об'єктів за багатьма класами і з врахуванням імплементації його в архітектуру частково централізованих розподілених систем для отримання цілісного сенсору та прийнятті рішення щодо віднесення worm-вірусу до певного класу, що покращило достовірність виявлення на 8-11% порівняно з використанням методу без залучення безпосередньо елементів та компонентів системи.

Напрямами подальших досліджень буде доповнення в базу системи функцій, які можуть використовувати worm-віруси при своєму функціонуванні та узгодження часу відповіді між компонентами при виконанні завдань в них.

Література

1. Security information portal Virus Bulletin, threat landscape. Available online: https://www.virusbulletin.com/ (accessed on 8.01.2024).

2. The Independent IT-Security Institute. Available online: https://www.av-test.org/en/ (accessed on 8.01.2024)

3. Nicheporuk, A., Savenko, O., Nicheporuk, A., & Nicheporuk, Y. (2020, October). An Android Malware Detection Method Based on CNN Mixed-Data Model. In *ICTERI Workshops* (pp. 198-213)

4. Kashtalian, A., Lysenko, S., Savenko, B., Sochor, T., & Kysil, T. (2023). Principle and method of deception systems synthesizing for malware and computer attacks detection. *Radioelectronic and Computer Systems, 0*(4), 112-151. doi:https://doi.org/10.32620/reks.2023.4.10

5. Lysenko S., Savenko O., Bobrovnikova K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. CEUR-WS 2018, 2104, 688–695.

6. Bobrovnikova K., Lysenko S., Savenko B., Gaj P., Savenko O. Technique for IoT malware detection based on control flow graph analysis. Radioelectron. Comput. Syst. 2022, 1, 141–153.

7. Savenko B., Lysenko, S., Bobrovnikova K., Savenko O. Markowsky G. Detection DNS Tunneling Botnets. In Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Cracow, Poland, 22–25 September 2021; Volume 1, pp. 64–69.

8. Савенко Б. О. Розподілені системи виявлення зловмисного програмного забезпечення. *2022 International Conference on Innovative Solutions in Software Engineering (ICISSE-2022)* : Conference Proceedings. (Ivano-Frankivsk, Ukraine, November 29-30, 2022) / Kuz M., Kozenko M. eds. Ivano-Frankivsk: VSPNU, 2022. Pp. 22–25. URL: https://kit.pnu.edu.ua/wp-content/uploads/sites/70/2023/01/2022_International_Conference_on_Innovative_Solutions_in_Software.pdf

9. Савенко Б. О. Розподілена частково централізована система виявлення зловмисного програмного забезпечення в комп'ютерних мережах. *Актуальні проблеми комп'ютерних наук АПКН-2022»* : матеріали XIV всеукр. наук.-практ. конф. (м. Хмельницький, 18-19 лист. 2022 р.). Хмельницький, 2022. С. 251–253. URL: https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn2022_corpuspaper.pdf

10. США ліквідували шкідливе ПЗ Snake, за допомогою якого Росія 20 років шпигувала у країнах НАТО — Politico (zn.ua). URL: https://zn.ua/ukr/usa/ssha-likviduvali-shkidlive-prohramne-zabezpechennja-snake-za-dopomohoju-jakoho-rosija-20-rokiv-shpihuvala-v-krajinakh-nato.html (accessed on 26.01.2024)

11. TrendMicro, https://www.trendmicro.com/vinfo/us/security/news/ botnets (accessed January 10, 2024).

12. Zeek, https:// https://zeek.org (accessed January 26, 2024).

13. Савенко Б. О. Метод синтезу математичних моделей рівнів безпеки для частково централізованих розподілених систем виявлення зловмисного програмного забезпечення. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки,* 2023. №3, Ч.1. С. 217-227. DOI: http://www.tech.vernadskyjournals.in.ua/journals/2023/3_2023/part_1/34.pdf

14. Murthy J.K. A Functional Decomposition of Virus and Worm Programs. In: Qing, S., Gollmann, D., Zhou, J. (eds) Information and Communications Security. ICICS 2003. *Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg. 2003. Vol. 2836. Pp. 405-414. https://doi.org/10.1007/978-3-540-39927-8_37

15. Desmedt Y. Trojan Horses, Computer Viruses, and Worms. In: van Tilborg, H.C.A., Jajodia, S. (eds) *Encyclopedia of Cryptography and Security.* Springer, Boston, MA. 2011. Pp. 1319–1320. https://doi.org/10.1007/978-1-4419-5906-5_331

16. Sheikh A. Trojans, Backdoors, Viruses, and Worms. In: Certified Ethical Hacker (CEH) *Preparation Guide*. Apress, Berkeley, CA. 2021. 217 p. https://doi.org/10.1007/978-1-4842-7258-9_5

17. Shaojie W., Qiming L. Analysis of a Mathematical Model for Worm Virus Propagation. Advances in Information Security and Its Application. ISA 2009. *Communications in Computer and Information Science*. Springer, Berlin, Heidelberg. 2009. Vol. 36. Pp. 78-84. https://doi.org/10.1007/978-3-642-02633-1_10

18. Pham VH., Dacier M., Urvoy-Keller G., En-Najjary T. The Quest for Multi-headed Worms. In: Zamboni, D. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2008. *Lecture Notes in Computer Science.* Springer, Berlin, Heidelberg. 2008. Vol. 5137. Pp. 247–266. https://doi.org/10.1007/978-3-540-70542-0_13

19. Ngo F.T., Agarwal A., Govindu R., MacDonald C. Malicious Software Threats. In: *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham. 2019. Pp. 1-22. https://doi.org/10.1007/978-3-319-90307-1_35-1

20. Edge C., Barker W., Hunter B., Sullivan G. Malware Security: Combating Viruses, Worms, and Root Kits. In: *Enterprise Mac Security*. Apress. 2010. Pp. 213–232. https://doi.org/10.1007/978-1-4302-2731-1_8

21. Znaj.ua. Видалити не можна залишити: путінські хакери народили небезпечний вірус [Електронний ресурс]: [Веб-сайт]. – Електронні дані – Режим доступу: https://znaj.ua/world/177015-vidaliti-ne-mozhna-zalishiti-putinski-hakeri-narodili-nebezpechniy-virus (дата звернення 27.01.2024). – Назва з екрану.

22. G. Markowsky, O. Savenko, S. Lysenko, A. Nicheporuk, The Technique for Metamorphic Viruses' Detection Based on its Obfuscation Features Analysis, CEUR Workshop Proceedings, Vol. 2104, 2018, pp. 680-687.

23. Zashcholkin, K., Drozd, O., Sulima, Y., Ivanova, O., & Perebeinos, I. (2020). DETECTION METHOD OF THE PROBABLE INTEGRITY VIOLATION AREAS IN FPGA-BASED SAFETY-CRITICAL SYSTEMS. *International Journal of Computing*, *19*(2), 282-289. https://doi.org/10.47839/ijc.19.2.1772

24. Zashcholkin K. The detection method of probable areas of hardware Trojans location in FPGA-based components of safety-critical systems / K. Zashcholkin, O. Drozd, // Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018. – 2018. – Pp. 212-217.

25. Адаптивна інформаційна технологія діагностування комп'ютерних систем на наявність троянських програм: автореф. дис. ... канд. техн. наук : 05.13.06 / С. М. Лисенко ; Терноп. нац. екон. ун-т. — Т., 2010. — 20 с.: а-рис. — укр.

26. Savenko O. The Technique for Computer Systems Trojan Diagnosis in the Monitor Mode / O. Savenko S. Lysenko // Proceedings of the 6-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Prague (Czech Republic), September 15-17, 2011. – Pp. 770-774.

27. Мультиагентна інформаційна технологія діагностування комп'ютерних систем на наявність бот-мереж у корпоративних мережах [Текст] : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.06 - інформаційні технології / Крищук Андрій Федорович. – Тернопіль : ТНЕУ, 2015. – 20 с. http://library.wunu.edu.ua/libsearch/DocDescription?doc_id=315623

28. Дудикевич В. Б. Квінтесенція інформаційної безпеки кіберфізичної системи / В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець // Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. — Львів: Видавництво Львівської політехніки, 2018. – № 887. – С. 58–68.

29. Sochor T. Behavioral Analysis of Bot Activity in Infected Systems Using Honeypots/ M. Zuzcak, T. Sochor// Proceedings of the 24-st International Conference on Computer Networks. – Springer (Cham), May 30, 2017, Vol. 718. – Pp. 118-133.

30. Martynyuk O. Evolutionary Network Model of Testing of the Distributed Information Systems / O. Martynyuk, A. Sugak, D. Martynyuk, O. Drozd // Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017. – 2017. – Vol. 2. - Pp. 888-893.

31. What is a Wireless Intrusion Prevention System (WIPS)? Wi-Fi Security That's No Longer Up in the Air. Available online: https://www.justfirewalls.com/what-is-a-wireless-intrusion-prevention-system/.(accessed on 12.04.2023).

32. Hossein Ashtari. What Is Network Behavior Analysis? Definition, Importance, and Best Practices. Network behavior analysis solutions collect and analyze enterprise network data to identify unusual activity and

counter security threats. Available online: https://www.spiceworks.com/tech/networking/articles/network-behavior-analysis/.(accessed on 12.04.2023).

33. Савченко А.С. Методи розподіленого управління корпоративними комп'ютерними мережами. – Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 «Інформаційні технології». – Національний авіаційний університет, Київ, 2021. – 341 с. https://er.nau.edu.ua/handle/NAU/48951?mode=full

34. ДСТУ ISO/IEC 2382-18:2005 Інформаційні технології. Словник термінів. Частина 18. Розподілене оброблення даних.

35. Корченко, А.О. Методи ідентифікації аномальних станів для систем виявлення вторгнень. Автореферат дисертації д-ра техн. наук: 05.13.21, Національний авіаційний університет, Київ, 2019, с 40.

36. Sergii Lysenko. Detection of the botnets' low-rate DDoS attacks based on self-similarity / Lysenko, S., Bobrovnikova, K., Matiukh, S., Hurman, I., Savenko, O. // International Journal of Electrical and Computer Engineering. – 2020. – Vol. 10., №4 – PP.-3651-3659, ISSN: 2088-8708.

37. S. Lysenko, O. Savenko, K. Bobrovnikova, A. Kryshchuk. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks / Communications in Computer and Information Science, 2018.- 860, - Pp. 385-401.

38. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko, "Malware Detection By Distributed Systems with Partial Centralization," *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS),* Dortmund, Germany, 2023, pp. 265-270, doi: 10.1109/IDAACS58523.2023.10348773.

39. Sergii Lysenko. BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks / Sergii Lysenko, Kira Bobrovnikova, Oleg Savenko and Andrii Kryshchuk // Communications in Computer and Information Science. – 2019. – Vol. 1039. – PP.-127-143, ISSN: 1865-0929.

40. Лисенко С.М. Методологічні основи та інформаційна технологія забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз –Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 «Інформаційні технології» (12 – Інформаційні технології) –Українська академія друкарства, Львів, 2020. - 409 с.

41. Стецюк М. В. Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення. – Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія. – Хмельницький національний університет, Хмельницький, 2022. – 249 с. https://nauka.khmnu.edu.ua/wp-content/uploads/dysertacziya-1.pdf

42. Khoroshko V., Khokhlachova Y., Vyshnevska N. Choice of indicators for forecasting cyber protection of computer systems Ukrainian Scientific Journal of Information Security Vol. 29 No. 1 (2023): C. 41-47.

43. Kharchenko, V.; Ponochovnyi, Y.; Ivanchenko, O.; Fesenko, H.; Illiashenko, O. Combining Markov and Semi-Markov Modelling for Assessing Availability and Cybersecurity of Cloud and IoT Systems. *Cryptography* **2022**, *6*, 44. https://doi.org/10.3390/cryptography6030044

44. Лукова-Чуйко, Н.В. Методологічні основи забезпечення функціональної стійкості розподілених інформаційних систем до кібернетичних загроз: автореферат дисертації д-ра техн. наук: 05.13.06, Державний університет телекомунікацій, Київ, 2018, с. 40.

45. Zillya Антивірус, https://zillya.ua/index.php?q=worm (accessed on 27.01.2024).

46. Б. Савенко, А. Каштальян, Н. Петляк. Розподілені системи виявлення worm-вірусів. *2023 ITSec: Безпека інформаційних технологій:* Матеріали XII Міжнар. наук.-техн. конф. (м. Ужгород, 2-4 трав. 2023 р. К.: НАУ). 2023. С. 37-39. http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf

47. Вірус вразив тисячі комп'ютерів. *Gazeta.ua*. 02 листопада 2023 (accessed January 27, 2024). https://gazeta.ua/articles/edu-and-science/_virus-vraziv-tisyachi-kompyuteriv/867493

48. Lysenko, S. and Savenko, B. 2023. Distributed Discrete Malware Detection Systems Based on Partial Centralization and Self-Organization. *International Journal of Computing*. 22, 2 (Jul. 2023), 117-139. DOI: https://doi.org/10.47839/ijc.22.2.3082

References

1. Security information portal Virus Bulletin, threat landscape. Available online: https://www.virusbulletin.com/ (accessed on 8.01.2024).

2. The Independent IT-Security Institute. Available online: https://www.av-test.org/en/ (accessed on 8.01.2024)

3. Nicheporuk, A., Savenko, O., Nicheporuk, A., & Nicheporuk, Y. (2020, October). An Android Malware Detection Method Based on CNN Mixed-Data Model. In *ICTERI Workshops* (pp. 198-213)

4. Kashtalian, A., Lysenko, S., Savenko, B., Sochor, T., & Kysil, T. (2023). Principle and method of deception systems synthesizing for malware and computer attacks detection. *Radioelectronic and Computer Systems, 0*(4), 112-151. doi:https://doi.org/10.32620/reks.2023.4.10

5. Lysenko S., Savenko O., Bobrovnikova K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. CEUR-WS 2018, 2104, 688–695.

6. Bobrovnikova K., Lysenko S., Savenko B., Gaj P., Savenko O. Technique for IoT malware detection based on control flow graph analysis. Radioelectron. Comput. Syst. 2022, 1, 141–153.

7. Savenko B., Lysenko, S., Bobrovnikova K., Savenko O. Markowsky G. Detection DNS Tunneling Botnets. In Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Cracow, Poland, 22–25 September 2021; Volume 1, pp. 64–69.

8. Savenko B. O. Distributed malware detection systems. *2022 International Conference on Innovative Solutions in Software Engineering (ICISSE-2022)* : Conference Proceedings. (Ivano-Frankivsk, Ukraine, November 29-30, 2022) / Kuz M., Kozenko M. eds. Ivano-Frankivsk:

VSPNU, 2022. Pp. 22–25. URL: https://kit.pnu.edu.ua/wp-content/uploads/sites/70/2023/01/2022_International_Conference_on_Innovative_Solutions_in_Software.pdf (In Ukrainian)

9. Savenko B. O. A distributed, partially centralized system for detecting malicious software in computer networks. Actual problems of computer science APKN-2022: materials of the XIV All-Ukrainian Conference. science and practice conf. (Khmelnytskyi, November 18-19, 2022). Khmelnytskyi, 2022. C. 251–253. URL: https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn2022_corpuspaper.pdf (In Ukrainian)

10. The US has eliminated the Snake malware, which Russia used to spy on NATO countries for 20 years — Politico (zn.ua). URL: https://zn.ua/ukr/usa/ssha-likviduvali-shkidlive-prohramne-zabezpechennja-snake-za-dopomohoju-jakoho-rosija-20-rokiv-shpihuvala-v-krajinakh-nato.html (accessed on 26.01.2024) (In Ukrainian)

11. TrendMicro, https://www.trendmicro.com/vinfo/us/security/news/ botnets (accessed January 10, 2024).

12. Zeek, https:// https://zeek.org (accessed January 26, 2024).

13. Savenko B. O. Method of synthesis of mathematical models of security levels for partially centralized distributed systems of detection of malicious software. Academic notes of the Tavri National University named after V.I. Vernadskyi. Series: Technical sciences, 2023. No. 3, Part 1. Pp. 217-227. DOI: http://www.tech.vernadskyjournals.in.ua/journals/2023/3_2023/part_1/34.pdf (In Ukrainian)

14. Murthy J.K. A Functional Decomposition of Virus and Worm Programs. In: Qing, S., Gollmann, D., Zhou, J. (eds) Information and Communications Security. ICICS 2003. *Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg. 2003. Vol. 2836. Pp. 405-414. https://doi.org/10.1007/978-3-540-39927-8_37

15. Desmedt Y. Trojan Horses, Computer Viruses, and Worms. In: van Tilborg, H.C.A., Jajodia, S. (eds) *Encyclopedia of Cryptography and Security.* Springer, Boston, MA. 2011. Pp. 1319–1320. https://doi.org/10.1007/978-1-4419-5906-5_331

16. Sheikh A. Trojans, Backdoors, Viruses, and Worms. In: Certified Ethical Hacker (CEH) *Preparation Guide*. Apress, Berkeley, CA. 2021. 217 p. https://doi.org/10.1007/978-1-4842-7258-9_5

17. Shaojie W., Qiming L. Analysis of a Mathematical Model for Worm Virus Propagation. Advances in Information Security and Its Application. ISA 2009. *Communications in Computer and Information Science*. Springer, Berlin, Heidelberg. 2009. Vol. 36. Pp. 78-84. https://doi.org/10.1007/978-3-642-02633-1_10

18. Pham VH., Dacier M., Urvoy-Keller G., En-Najjary T. The Quest for Multi-headed Worms. In: Zamboni, D. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2008. *Lecture Notes in Computer Science.* Springer, Berlin, Heidelberg. 2008. Vol. 5137. Pp. 247–266. https://doi.org/10.1007/978-3-540-70542-0_13

19. Ngo F.T., Agarwal A., Govindu R., MacDonald C. Malicious Software Threats. In: *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham. 2019. Pp. 1-22. https://doi.org/10.1007/978-3-319-90307-1_35-1

20. Edge C., Barker W., Hunter B., Sullivan G. Malware Security: Combating Viruses, Worms, and Root Kits. In: *Enterprise Mac Security*. Apress. 2010. Pp. 213–232. https://doi.org/10.1007/978-1-4302-2731-1_8

21. Znaj.ua. Delete cannot be left: Putin's hackers gave birth to a dangerous virus [Electronic resource]: [Website]. – Electronic data – Access mode: https://znaj.ua/world/177015-vidaliti-ne-mozhna-zalishiti-putinski-hakeri-narodili-nebezpechniy-virus (accessed on 7.01.2024). – Name from the screen. (In Ukrainian)

22. G. Markowsky, O. Savenko, S. Lysenko, A. Nicheporuk, The Technique for Metamorphic Viruses' Detection Based on its Obfuscation Features Analysis, CEUR Workshop Proceedings, Vol. 2104, 2018, pp. 680-687.

23. Zashcholkin, K., Drozd, O., Sulima, Y., Ivanova, O., & Perebeinos, I. (2020). DETECTION METHOD OF THE PROBABLE INTEGRITY VIOLATION AREAS IN FPGA-BASED SAFETY-CRITICAL SYSTEMS. *International Journal of Computing*, *19*(2), 282-289. https://doi.org/10.47839/ijc.19.2.1772

24. Zashcholkin K. The detection method of probable areas of hardware Trojans location in FPGA-based components of safety-critical systems / K. Zashcholkin, O. Drozd, // Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018. – 2018. – Pp. 212-217.

25. Adaptive information technology for diagnosing computer systems for the presence of Trojan programs: autoref. thesis ... candidate technical Sciences: 05.13.06 / S. M. Lysenko; Ternopil national economy Univ. — T., 2010. — 20 p. (In Ukrainian)

26. Savenko O. The Technique for Computer Systems Trojan Diagnosis in the Monitor Mode / O. Savenko S. Lysenko // Proceedings of the 6-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Prague (Czech Republic), September 15-17, 2011. – Pp. 770-774.

27. Multi-agent information technology for diagnosing computer systems for the presence of bot networks in corporate networks [Text]: autoref. thesis for obtaining sciences. candidate degree technical Sciences: spec. 05.13.06 - information technologies / Andriy Fedorovych Kryshchuk. – Ternopil: TNEU, 2015. – 20 p. http://library.wunu.edu.ua/libsearch/DocDescription?doc_id=315623 (In Ukrainian)

28. Dudykevich V. B. The quintessence of information security of a cyber-physical system / V. B. Dudykevich, G. V. Mykytin, A. I. Rebets // Bulletin of the National University "Lviv Polytechnic". Information systems and networks. — Lviv: Lviv Polytechnic Publishing House, 2018. – № 887. – Pp. 58–68. (In Ukrainian)

29. Sochor T. Behavioral Analysis of Bot Activity in Infected Systems Using Honeypots/ M. Zuzcak, T. Sochor// Proceedings of the 24-st International Conference on Computer Networks. – Springer (Cham), May 30, 2017, Vol. 718. – Pp. 118-133.

30. Martynyuk O. Evolutionary Network Model of Testing of the Distributed Information Systems / O. Martynyuk, A. Sugak, D. Martynyuk, O. Drozd // Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017. – 2017. – Vol. 2. - Pp. 888-893.

31. What is a Wireless Intrusion Prevention System (WIPS)? Wi-Fi Security That's No Longer Up in the Air. Available online: https://www.justfirewalls.com/what-is-a-wireless-intrusion-prevention-system/.(accessed on 12.04.2023).

32. Hossein Ashtari. What Is Network Behavior Analysis? Definition, Importance, and Best Practices. Network behavior analysis solutions collect and analyze enterprise network data to identify unusual activity and counter security threats. Available online: https://www.spiceworks.com/tech/networking/articles/network-behavior-analysis/.(accessed on 12.04.2023).

33. Savchenko A.S. Methods of distributed management of corporate computer networks. - Dissertation for obtaining the scientific degree of Doctor of Technical Sciences in the specialty 05.13.06 "Information technologies". – National Aviation University, Kyiv, 2021. – 341 p. https://er.nau.edu.ua/handle/NAU/48951?mode=full (In Ukrainian)

34. DSTU ISO/IEC 2382-18:2005 Information technologies. Dictionary of terms. Part 18. Distributed data processing. (In Ukrainian)

35. Korchenko, A.O. Methods of identifying abnormal states for intrusion detection systems. Abstract of the dissertation of Dr. Tech. Sciences: 05.13.21, National Aviation University, Kyiv, 2019, 40 p.

36. Sergii Lysenko. Detection of the botnets' low-rate DDoS attacks based on self-similarity / Lysenko, S., Bobrovnikova, K., Matiukh, S., Hurman, I., Savenko, O. // International Journal of Electrical and Computer Engineering. – 2020. – Vol. 10., №4 – PP.-3651-3659, ISSN: 2088-8708.

37. S. Lysenko, O. Savenko, K. Bobrovnikova, A. Kryshchuk. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks / Communications in Computer and Information Science, 2018.- 860, - Pp. 385-401.

38. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko, "Malware Detection By Distributed Systems with Partial Centralization," *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS),* Dortmund, Germany, 2023, pp. 265-270, doi: 10.1109/IDAACS58523.2023.10348773.

39. Sergii Lysenko. BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks / Sergii Lysenko, Kira Bobrovnikova, Oleg Savenko and Andrii Kryshchuk // Communications in Computer and Information Science. – 2019. – Vol. 1039. – PP.-127-143, ISSN: 1865-0929.

40. Lysenko S.M. Methodological foundations and information technology for ensuring the resilience of computer systems in the face of cyber threats - Dissertation for obtaining the scientific degree of Doctor of Technical Sciences 05.13.06 "Information technologies" (12 - Information technologies) - Ukrainian Academy of Printing, Lviv, 2020. - 409 p. (In Ukrainian)

41. Stetsyuk M. V. Methods and means of ensuring failure resistance and survivability of specialized information technologies under the influence of malicious software. - Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 123 - Computer Engineering. – Khmelnytskyi National University, Khmelnytskyi, 2022. – 249 p. https://nauka.khmnu.edu.ua/wp-content/uploads/dysertacziya-1.pdf (In Ukrainian)

42. Khoroshko V., Khokhlachova Y., Vyshnevska N. Choice of indicators for forecasting cyber protection of computer systems Ukrainian Scientific Journal of Information Security Vol. 29 No. 1 (2023): C. 41-47.

43. Kharchenko, V.; Ponochovnyi, Y.; Ivanchenko, O.; Fesenko, H.; Illiashenko, O. Combining Markov and Semi-Markov Modelling for Assessing Availability and Cybersecurity of Cloud and IoT Systems. *Cryptography* **2022**, *6*, 44. https://doi.org/10.3390/cryptography6030044

44. Lukova-Chuiko, N.V. Methodological foundations of ensuring the functional stability of distributed information systems against cyber threats: abstract of the dissertation of Dr. Tech. Sciences: 05.13.06, State University of Telecommunications, Kyiv, 2018, p. 40. (In Ukrainian)

45. Zillya Антивірус, https://zillya.ua/index.php?q=worm (accessed on 27.01.2024).

46. B. Savenko, A. Kashtalyan, N. Petlyak. Distributed worm detection systems. 2023 ITSec: Security of information technologies: Proceedings of the 12th International science and technology conf. (Uzhgorod, May 2-4, 2023. K.: NAU). 2023. P. 37-39. http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf (In Ukrainian)

47. The virus affected thousands of computers. *Gazeta.ua*. 02.11.2023 (accessed January 27, 2024). https://gazeta.ua/articles/edu-and-science/_virus-vraziv-tisyachi-kompyuteriv/867493 (In Ukrainian)

48. Lysenko, S. and Savenko, B. 2023. Distributed Discrete Malware Detection Systems Based on Partial Centralization and Self-Organization. *International Journal of Computing*. 22, 2 (Jul. 2023), 117-139. DOI: https://doi.org/10.47839/ijc.22.2.3082