КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІ, СИСТЕМНИЙ АНАЛІЗ ТА КІБЕРБЕЗПЕКА

DOI 10.31891/2307-5732-2020-289-5-45-50
УДК 004.75:004.8:004.49

А.С. КАШТАЛЬЯН, Б.О. САВЕНКО, В.І. ГРИБИНЧУК
Хмельницький національний університет

МОДЕЛІ ТА ТИПИ ПРИМАНОК ДЛЯ ЗЛОВМИСНИХ АТАК В КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

В статті розроблені моделі приманок, мереж приманок та аналіз особливостей типів приманок дають змогу вибудувати систему хибних об'єктів атак, інтегровану в загальну систему безпеки корпоративних мереж, що загалом сприятиме покращенню рівня безпеки. Моделі приманок та мереж приманок є основою для розробки принципово нових методів виявлення зловмисного втручання в функціонування корпоративних мереж. Особливістю є досягнення за рахунок конфігурування різних типів приманок та їх інтеграції не тільки з іншими системами забезпечення рівня безпеки корпоративних мережах і за рахунок їх представлення в багаторівневій системі, яка за своєю архітектурою буде здійснювати ефективну реакцію на зловмисні події. В роботі представлено типові особливості приманок та враховано їх в розроблених формалізованих представленнях моделей приманок і їх мереж. Результати експериментальних досліджень представлені на основі характеристики побудованої мережі приманок в багаторівневій системі, яка динамічно змінюватиме свою конфігурацію та матиме систему прийняття рішень для оперативного реагування на події, що протікатимуть в мережі. В роботі показано застосування приманок як перспективний напрям у боротьбі із зловмисними втручаннями в роботу корпоративних мереж, інформація про які обмежена або відсутня. Розроблені в роботі моделі приманок та мереж приманок дають змогу вибудувати систему хибних об'єктів атак, інтегровану в загальну систему безпеки корпоративних мереж, що загалом сприятиме покращенню рівня безпеки.

Ключові слова: мережа приманок, зловмисні дії, виявлення комп'ютерних атак, прогнозування, корпоративні комп'ютерні мережі.

A. KASHTALIAN, B. SAVENKO, V. GRIBINCHOOK
Khmelnytskyi National University

MODELS AND TYPES OF Honeypots FOR MALICIOUS ATTACKS IN CORPORATE COMPUTER NETWORKS

The models of baits, bait networks and analysis of the features of the types of baits developed in the article make it possible to build a system of false objects of attack, integrated into the general security system of corporate networks, which will generally improve security. Models of lures and bait networks are the basis for the development of fundamentally new methods of detecting malicious interference in the functioning of corporate networks. This is achieved by configuring different types of lures and integrating them not only with other systems to ensure the level of security of corporate networks and by presenting them in a multilevel system, which by its architecture will effectively respond to malicious events. The paper presents typical features of baits and takes them into account in the developed formalized representations of bait models and their networks. The results of experimental research are presented on the basis of the characteristics of the constructed network of lures in a multilevel system, which will dynamically change its configuration and have a decision-making system for rapid response to events occurring in the network. The paper shows the use of baits as a promising direction in the fight against malicious interference in the work of corporate networks, information about which is limited or absent. The models of lures and lure nets developed in the work allow to build a system of false objects of attack, integrated into the general security system of corporate networks, which will generally help to improve the level of security.

Keywords: honeynet, malicious actions, detection of computer attacks, forecasting, corporate computer networks.

Вступ. Постановка проблеми

Використання комп'ютерних мережних ресурсів в роботі підприємств (організацій) стало невід'ємною частиною забезпечення технологічних процесів, що протікають в них. Але комп'ютерні мережі мають такі особливості, що будучи під'єднаними до мережі Internet стають об'єктами для зловмисних дій [1]. Для виявлення зловмисних дій та захисту від них використовується багато різного типу та призначення систем. Зокрема, захист інформаційних ресурсів мереж вирішуються за допомогою брандмауерів (firewall), антивірусів, систем виявлення атак (Intrusion Detection System, IDS), систем контролю цілісності, криптографічних засобів захисту [2].

Існуючі системи забезпечення захисту корпоративних мереж не забезпечують надійного захисту. Тому, актуальним напрямом дослідження є пошук більш ефективних шляхів виявлення зловмисних дій в роботі мережі. Основною вимогою до таких підходів є можливість виявлення будь-яких типів зловмисних втручань, в тому числі і нових, а також впливів, розподілених у часі. Перспективним напрямом для виявлення нових типів загроз є використання окремих приманок та їх приманок в комп'ютерних мережах, а також їх інтеграція з іншими системами захисту. Метою дослідження є розробка моделей приманок та їх мереж на основі аналізу їх типів та особливостей застосування.

1. Методи виявлення зловмисних дій на основі приманок та мереж приманок

Приманки у локальних мережах та мережі Інтернет виконують функції збору та аналізу інформації щодо зловмисних дій в мережах [3–5]. Актуальними напрямами дослідження є розміщення приманок саме в

корпоративних мережах для покращення безпеки в них. Розглянемо методи побудови таких приманок, які орієнтовані саме на використання в корпоративних комп'ютерних мережах підприємств (організацій).

В роботах [6, 7] приведено результати використання мережі, що містить невелику кількість низькорівневих приманок, які дозволяють здійснювати пряме вимірювання атак та їх походження. Висновок здійснюється на основі статистичного аналізу.

Приманки описані в [7] двох типів: низькорівневі та високорівневі, які призначені для виявлення загроз сервісам з операційними системами Linux та Windows. Вони є клієнтські та серверні і реалізовані на різних мовах програмування. Перспективним спрямування використання приманок авторами пропонується ряд додаткових інструментів, дотичних до приманок, зокрема інструменти, що розширюють функціональність приманок та мереж та інструменти для виявлення приманок.

Використання тіньових приманок пропонується в [8, 9]. Вони представляють собою гібридну архітектуру, що поєднує ознаки приманок та систем виявлення втручань. Тіньова приманка розділяє всі внутрішні стани робочого сервісу і здатна виявляти потенційні загрози. Таким чином, атаки підтверджені приманкою, відфільтровуються, а нормальний трафік, помилково класифікований як аномальний, опрацьовується коректно. Вихідні дані з тіньової приманки надалі використовуються для подальшого вдосконалення систем виявлення втручань, зменшуючи кількість хибно позитивних результатів.

Метод на основі застосування приманок до виявлення зловмисних дій, який змінює їх пасивну роль очікування атак на активне ефективне використання у взаємодії приманок та мережі, в якій вони розгорнуті, запропоновано в роботі [10]. Це передбачає розпізнавання зловмисних дій на їх початковому етапі та перенаправлення мережного трафіку на приманку до того як зловмисні дії завдадуть реальної школи.

Віртуалізація відіграє значну роль в останніх трендах хмарних обчислень та зберігання даних, що ускладнює задачу одночасного надання якісного сервісу та захисту від втручань. Використання приманок у віртуальних середовищах для попередження зловмисних дій та реагування на них запропоновано в [11]. Віртуальні приманки та мережі віртуальних приманок дозволяють зменшити витрати у порівнянні з фізичними приманками [12].

Підключення локальних пристроїв різноманітних пристроїв, в тому числі це стосується інтернету речей до таких мереж несе в собі загрозу не тільки доступу до даних, а також безпосереднього втручань в роботу цих пристроїв. Для збереження конфіденційності інформації та запобігання втручань в роботу використовуються приманки [13].

Приманки можуть бути ідентифіковані зловмисниками з використанням різних методів [13]. Ці підходи досліджуються та моделюються з метою захисту та здійснення контрзаходів щодо виявлення приманок [15, 16]. Для автоматичної ідентифікації приманок використовуються сучасні методи, в тому числі методи машинного навчання, такі як дерева рішень та випадковий ліс [17].

2. Відомі типи приманок для виявлення зловмисних дій та їх моделі

Розглянемо типи розповсюджених приманок для виявлення зловмисних в комп'ютерних мережах. Побудуємо моделі приманок на основі групування і узагальнення їх характеристик з метою створення мереж приманок в корпоративних комп'ютерних мережах для покращення рівнів безпеки в них.

В табл. 1 надано рівні роботи приманок з урахуванням її функцій.

Таблиця 1

Рівні роботи приманок

Рівень	Виконувані функції
Рівень виявлення	Збір мережного трафіку, повідомлення виявлення приманки зловмисником
Рівень аналізу	Аналіз та оцінка дій зловмисника, аналіз виявлення приманки зловмисником
Рівень реагування	Реагування на дії зловмисника
Рівень виконання	Виявлення атак, попередження зловмисних дій

Рівень виявлення забезпечує збір інформації щодо втручань в роботу сервісу. До цієї інформації відносяться дані щодо виявлення приманки зловмисником, виявлення портів, що прослуховують сервер, виявлення неавторизованих облікових записів, виявлення файлів, заміщених зловмисником і т.п.

На рівні аналізу зібрана інформація аналізується, визначається яка саме зафіксована активність є зловмисною та визначається рівень її небезпеки для мережі. Рівень небезпеки зловмисних дій асоціюється з рівнем шкоди, що може бути завдана мережі. Наприклад, чи були зафіксовані дії неавторизованих користувачів, модифікації файлів тощо.

На рівні реагування формуються правила попередження та виявлення атак, сформовані на основі зібраної та проаналізованої інформації, які надалі використовуються мережею.

Рівень виконання поєднує дві основних функції. На етапі виявлення за відомими характеристиками (сигнатурами) виявляються атаки мережі на основі статичних патернів. На етапі попередження ці атаки блокуються як зловмисні.

Процес збору та аналізу інформації та реагування є неперервним. Правила виявлення динамічно оновлюються на основі інформації рівня виявлення та аналізу, що дозволяє постійно реагувати на нові види зловмисних дій та їх модифікації.

Задамо модель приманки на основі функцій, які вона виконує, та відношення «багато до одного». В даному відношенні приманка виступає одиничним об'єктом до якого можуть спрямовуватись атаки з різних

джерел. Нехай P – множина, яка позначає сукупність функцій приманки, причому функції можуть відноситись до різних рівнів і можуть дублюватись. Введемо операції на множині P, суть яких полягатиме в поєднанні модулів приманки різного призначення. Множина таких операцій на множині P надає можливість представляти модель приманки на основі функцій, з яких вона утворюється та врахувати різноманіття таких функцій. Позначимо цю множину Ω_P. Введемо множину предикатів Ω_I на множині P, які будуть істинними якщо операції з множини Ω_P виконуватимуться. Тоді задамо алгебраїчну структуру $\mathfrak{A}_P$ типу $\tau = (1, 1)$, яка поєднає всі розглянути множини для формування формалізованого представлення приманки:

$$\mathfrak{A}_P = \langle P, \Omega_P, \Omega_I \rangle, \quad (1)$$

де P – множина, яка позначає сукупність функцій приманки; Ω_P – множина таких операцій на множині P; Ω_I – множину предикатів на множині P.

Тоді модель приманки, яка враховуватиме функції з яких вона формуватиметься, задамо так:

$$\mathfrak{W}_P = \langle P, \Omega_I \rangle, \quad (2)$$

де P – множина, яка позначає сукупність функцій приманки; Ω_I – множину предикатів на множині P.

Розглянемо типи приманок за їх різними характеристиками. В табл. 2 відображено основні типи приманок та їх коротку характеристику.

Таблиця 2

Характеристика типів приманок

За використанням	
Виробничі (продукційні) приманки	Призначені для використання в реальних виробничих середовищах. Розташовуються всередині виробничої мережі з іншими виробничими серверами для підвищення загального рівня безпеки. Виробничі приманки є простими у використанні, потребують менше функціональності, ніж дослідницькі приманки, але й надають менше інформації про атаки та зловмисників.
Дослідницькі приманки	Основною метою використання цього типу приманок є збір та дослідження інформації щодо зловмисних втручання. Такі приманки безпосередньо не підвищують рівень безпеки середовища, в якому працюють. Натомість вони досліджують загрози, з якими стикається система, для подальшого захисту від них. Дослідницькі приманки зазвичай є складними у створенні та розгортанні. Однак відслідковують більше типів атак та надають про них більше інформації.
За рівнем взаємодії	
Низького рівня взаємодії	Такий тип приманок характеризується мінімальною взаємодією з зловмисниками. Приманки не мають реальної операційної системи чи сервісів, тільки емулюють роботу певних серверів, наприклад, ftp або http. Відповідно, такі приманки є простими в розгортанні та підтримці, але відслідковують обмежену кількість дій зловмисників. Окремим підтипом є тіньові приманки, які працюють у взаємодії з системою виявлення втручань. Якщо система виявлення втручань виявляє атаку, то виявлений аномальний трафік перенаправляється на приманку замість блокування для подальшого аналізу.
Середнього рівня взаємодії	Приманки цього типу поєднують властивості приманок низького та високого рівнів взаємодії. Приманки також не мають реального середовища, але забезпечують відповіді на запити зловмисників за рахунок рівня віртуалізації. Це дозволяє отримувати більше інформації про зловмисників. Приманки є більш складними у розгортанні.
Високого рівня взаємодії	Такі приманки мають реальну операційну систему, забезпечують високий рівень взаємодії і мають характеристики реального сервісу, що приваблює зловмисників. Тому, такі приманки дозволяють зібрати найбільше інформації про втручання і в більшості використовуються як дослідницькі, особливо при визначенні нових загроз. Розгортання і підтримка таких приманок є найбільш складною у порівнянні з іншими типами.
За типом розгортання обладнання	
Фізичні приманки	Фізична приманка представляє собою окремий комп'ютер із запущеною операційною системою та сервісами, з якої приманка приєднана до мережі через одну IP адресу. Фізичні приманки є дорого вартісні та дещо обмежені через одну IP адресу. В більшості випадків фізичні приманки є дослідницькими.
Віртуальні приманки	Віртуальні приманки можуть розташовуватися на одній фізичній машині з іншими сервісами. Можливе розташування декількох віртуальних приманок на одній машині. Завдяки цьому віртуальні приманки відслідковують більшу кількість IP адрес та є дешевшими в розгортанні.
За роллю приманки	
Пасивні (Server Side)	Звичайні приманки є пасивними і не ініціюють обміну даними крім випадків відповідей на атаки зловмисника. Такі приманки доцільні при виявленні атак різного типу, збиранні та дослідженні інформації про втручання.
Активні (Client Side)	Метою активних приманок є пошук та виявлення зловмисних серверів. Попереднє виявлення зловмисних серверів дозволяє захистити вразливі додатки клієнта.

Для захисту комп'ютерної мережі системою приманок передбачається, що їх розташовують у місцях можливого зловмисного втручання. Відносно комп'ютерної мережі можна виділити зовнішнє розташування приманок, внутрішнє та в зоні ДМЗ. На рис. 1 зображена типова багаторівнева система приманок, яка включає множину інтелектуальних приманок, що виконують постійний моніторинг мережі.

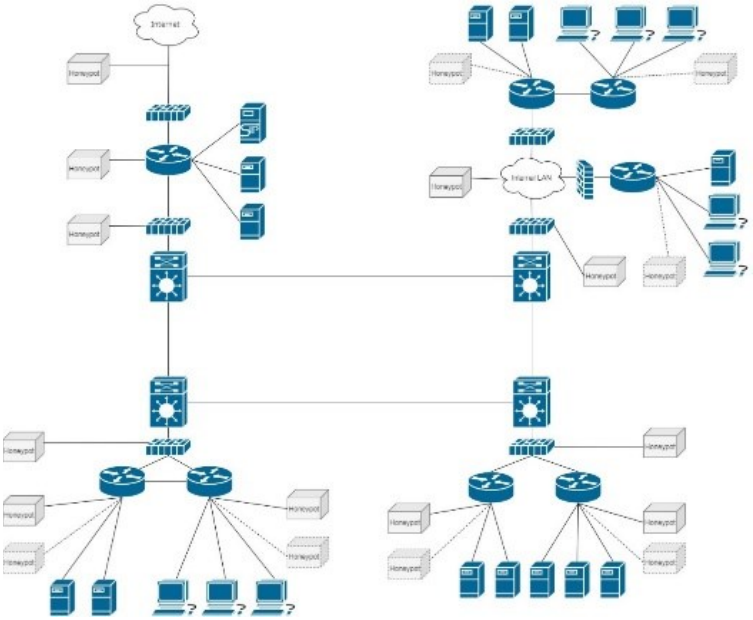

Рис. 1. Мережа з системою приманок

Така типова багаторівнева система приманок включає наступні типи приманок:

1. Зовнішні приманки, приєднані безпосередньо до мережі інтернет перед брандмауером. Ця приманка має найвищий рівень взаємодії, представляє собою фізичний сервіс з операційною системою, який емулює роботу реальних сервісів та відповідає на запити зловмисників. За рахунок цього, а також за рахунок розташування приманки у місці без будь якого захисту від втручань, приманка дає можливість зібрати максимально можливий об'єм інформації про дії зловмисників.

2. Приманки, розташовані в зоні ДМЗ. Ці приманки є фізичними і віртуальними, в залежності від їх кількості. Фізичні приманки працюють постійно під час роботи мережі. Віртуальні приманки можуть бути статичними і динамічними. Статичні приманки, так само як фізичні, працюють постійно. Динамічні приманки працюють підключаються за необхідності, якщо є потреба виявляти додаткові загрози або отримати більше інформації про дії зловмисників.

3. Основна множина приманок розташована всередині мережі і призначена для моніторингу безпеки сервісів та пристроїв підключених до мережі, в тому числі до внутрішньої локальної мережі. Так само як і в зоні ДМЗ всередині мережі використовується множина статичних та динамічних приманок, серед яких є фізичні та віртуальні.

Кількість статичних приманок та їх розташування в мережі фіксована.

Система приманок є мережею із своєю архітектурою та власною системою сервісів та фактично вбудована в мережу робочих сервісів, що значно підвищує контрольованість та захищеність системи в цілому. Елементами роботи мережі приманок є контроль даних, захоплення даних та збір даних.

Контроль даних системою приманок призначений зменшувати ризики здійснення атак щодо робочих сервісів, розміщених в мережі. Основною метою контролю дій зловмисника є швидке та ефективне реагування на них. Крім того, зловмиснику не повинно бути відомо, що його дії контролюються. Для зменшення ризиків система приманок повинна відповідати таким вимогам: контроль мережі має поєднувати ручний та автоматичний; для захисту від втручань необхідно щонайменше два рівні контролю даних; можливість підтримувати всі вхідні та вихідні з'єднання; можливість контролювати будь-яку несанкціоновану активність; здійснення контролю даних повинно конфігуруватися адміністратором в будь-який час; контроль зв'язку адміністратором повинен складно відслідковуватися зловмисником; наявність щонайменше двох методів попередження про зловмисну активність; можливість віддаленого адміністрування контролю даних; захоплення даних є наступною вимогою до мережі приманок і критично важливим є те, що захоплення активності приманкою має бути невідоме зловмиснику.

До захоплення даних мережею приманок висуваються такі вимоги: дані, захоплені приманкою, не зберігаються нею локально для того, щоб зловмисник не мав до них доступу; будь-який вплив інший даних не повинен впливати на процес захоплення даних приманкою; до активностей, які повинні відслідковуватися та фіксуватися, відносяться активності мережі, системи, додатків та користувачів; адміністратор повинен мати можливість віддалено відслідковувати роботу мережі приманок у реальному часі; захоплені дані повинні автоматично зберігатися для подальшого аналізу; інформація про захоплені дані повинна підтримуватися для кожної приманки мережі; адміністратор повинен виконувати оновлення приманок, які виявлені зловмисником; повинна забезпечуватися цілісність даних, захоплених мережею приманок.

Збір даних мережею приманок призначений для подальшого їх аналізу та інтеграції з даними про зловмисні дії, отримані з інших джерел. Ця інформація використовується для поточного та подальшого запобігання атакам. Для збору даних до мережі приманок висуваються вимоги: кожна приманка має унікальний ідентифікатор для взаємодії з мережею; можливість анонімізації даних, що стосуються приманок в мережі; обмін даними виконується із забезпеченням конфіденційності та цілісності даних; стандартизація та синхронізація обміну захопленими даними всередині мережі приманок.

Розглянута мережа може виконувати функцію поточного та перспективного захисту мережі від ряду зловмисних втручань, в тому числі від автоматизованих (автоматичних) атак та персоналізованих втручань.

Задамо модель мережі приманок на основі функцій, які вона виконує, та відношення «багато до багато» з використанням моделі (формула (1)). Модель мережі приманок, яка враховуватиме багаторівневість системи, в які вони використовуватимуться, задамо так:

$$\mathfrak{W} = \bigcup_P \mathfrak{W}_P, \tag{3}$$

де P – множина, яка позначає сукупність функцій приманки; $\mathfrak{W}_P$ – моделі приманок, сформовані з елементів множини P.

Розроблені моделі приманок, мереж приманок та аналіз особливостей типів приманок дають змогу вибудувати систему хибних об'єктів атак, інтегровану в загальну систему безпеки корпоративних мереж, що загалом сприятиме покращенню рівня безпеки. Моделі приманок та мереж приманок є основою для розробки принципово нових методів виявлення зловмисного втручання в функціонування корпоративних мереж. Це досягається за рахунок конфігурування різних типів приманок та їх інтеграції не тільки з іншими системами забезпечення рівня безпеки корпоративних мереж а і за рахунок їх представлення в багаторівневій системі, яка за своєю архітектурою буде здійснювати ефективну реакцію на зловмисні події.

3. Постановка експериментів з багаторівневою системою мережі приманок

Для розробки мереж приманок орієнтованих на використання в корпоративних мережах підприємств (організацій) необхідно розв'язати наступні задачі: встановити типові корпоративні мережі для яких буде використано пропоновану мережу приманок; визначитись із засобами захисту мережі, які будуть використовуватись; вибрати набір приманок різних типів для конфігурування мережі приманок; конфігурувати набір приманок в багаторівневу систему; провести узгодження взаємодії та уникнення конфліктів між стандартними використовуваними засобами захисту мережі та мережею приманок; здійснити активацію мережі приманок; провести первинне тестування стандартним набором тестів.

Проведення експериментальних досліджень з розробленою мережею приманок проводилось протягом тривалого часу (6 місяців) і мало на меті порівняння результатів з тими, які отримались без використання мережі приманок. Відсоткове покращення інтегрованого рівня безпеки в корпоративній мережі становило 3%. Його збільшення в перспективі є можливим за рахунок уточнення та покращення моделей приманок та комп'ютерних атак, а також покращення взаємодії компонентів багаторівневої системи.

Результати експериментальних досліджень дозволяють здійснити побудову мережі приманок, які динамічно змінюватимуть свою конфігурацію та матимуть систему прийняття рішень для оперативного реагування на події, що протікатимуть в мережі.

Висновки

Застосування приманок є перспективним напрямом у боротьбі із зловмисними втручаннями в роботу корпоративних мереж, інформація про які обмежена або відсутня. Розроблені моделі приманок та мереж приманок дають змогу вибудувати систему хибних об'єктів атак, інтегровану в загальну систему безпеки корпоративних мереж, що загалом сприятиме покращенню рівня безпеки. Результати експериментальних досліджень дозволяють здійснити побудову мережі приманок.

Напрямками подальших досліджень є удосконалення системи підтримки прийняття рішень в багаторівневій системі, яка включає в себе приманки, та покращення моделей приманок.

Література

1. Савенко О. С. Дослідження методів антивірусного діагностування комп'ютерних мереж / О. С. Савенко, С. М. Лисенко // Вісник Хмельницького національного університету. Технічні науки. – 2007. – № 2, т. 2. – С. 120–126.

2. Савенко О.С. Моделі незадокументованих закладок програмного забезпечення в локальних комп'ютерних мережах / О.С. Савенко, В.П. Паюк, Б.О. Савенко, А.С. Каштальян // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2019. – № 2. – С. 84–90.

3. Data Collection and Data Analysis in Honeypots and Honeynets. Pavol Sokol, Patrik Pekarčík, Tomáš Bajtoš. URL: http://spi.unob.cz/papers/2015/2015-19.pdf [Access 18.04.2020].

4. Study of Internet Threats and Attach Methods Using Honeypots and Honeynets. Tomas Sochor, Matej Zuzcak - Springer International Publishing Switzerland 2014, A. Kwiecie´n, P. Gaj, and P. Stera (Eds.): CN 2014, CCIS 431, p. 118–127, 2014.

5. Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection. Tomas Sochor, Matey Zuzcak – Springer International Publishing Switzerland 2015, P.Gaj at al. (Eds.): CN 2015, CCIS 522, p. 69-81, 2015. DOI: 10.1007/978-3-319-19419-6 7.

6. A Survey on Honeypot Software and Data Analysis. Marcin Nawrocki, Matthias Wählisch, Thomas C. Schmidt, Christian Keil, Jochen Schönfelder. arXiv:1608.06249v1 [cs.CR] 22 Aug 2016. URL: https://arxiv.org/abs/1608.06249 [Access 26.03.2020]

7. Composite Hybrid Techniques for Defending Against Targeted Attacks. S. Sidiroglou, A.D. Keromytis. Part of the Advanced in Information Security book series (ADIS, volume 27), 2007, 213-229 p.

8. Shadow Honeypots. K.G. Anagnostakis, S. Sidiroglou, M. Polychronakis, A.D. Keromytis, P. Markatos. International Journal of Computer and Network Security, Vol. 2, No. 9, September 2010, 16 p.

9. POSTER: Dragging Attackers to Honeypots for Effective Analysis of Cyber Threats. Martin Husak, Jan Vykopal. URL: https://is.muni.cz/repo/1188174/POSTER-Dragging_Attackers_to_Honeypots_for_Effective_Analysis_of_Cyber_Threats.pdf [Access 30.05.2020]

10. Effective Proactive and Reactive Defense Strategies against Malicious Attacks in a Virtualized Honeynet. Frank Yeong-Sung Lin, Yu-Shun Wang, Ming-Yang Huang. Journal of Applied Mathematics, Vol. 2013, Article ID 518213, 11 pages. URL: https://www.hindawi.com/journals/jam/2013/518213/ [Access 10.04.2020]

11. A Virtual Honeypot Framework. Niels Provos. URL: http://www.citi.umich.edu/u/provos/papers/honeyd.pdf [Access 12.04.2020]

12. Securing Internet of Things (IoT) Using HoneyPots. Sai Sudha Gadde, Rama Krishna Srinivas Ganta, ASALG Gopala Gupta, Raghava Rao K, KRR Mohan Rao. International Journal of Engineering & Technology, 7 (2.7), 2018, p. 820–824.

13. Enhancing Honeypot Deception Capability Through Network Service Fingerprinting. R.N. Dahbul, C. Lim, J. Purnama. Internation Conference on Computing and Applied Informatics 2019, Journal of Physics: Conf. Series 801. 2017.

14. Probabilistic Estimation of Honeypot Detection in Internet of Things Environment. O. Surnin, F. Hussain, R. Hussain, S. Ostrovskaya, A. Polovinkin, J.Y. Lee, X. Fernando. 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18-21 Feb. 2019, 191–196 p.

15. Automatic Identification of Honeypot Server Using Machine Learning Techniques. Cheng Huang, Jiaxuan Han, Xing Zhang, Jiayong Liu. Hindawi, Security and Communication Networks Volume 2019, Article ID 2627608, 8 pages.

16. Survey of Attach Projection, Prediction, and Forecasting in Cyber Security. Martin Husak, Jana Komarkova, Elias Bou-Harb, Pavel Celeda. IEEE Communication Survays & Tutorials – September 2018. URL: https://www.researchgate.net/publication/327449459_Survey_of_Attack_Projection_Prediction_and_Forecasting_in_Cyber_Security [Access 12.05.2020]

17. Honeypots and Routers: Collecting Internet Attacks. Mohssen Mohammed, Habib-ur Rehman – CRC Press, Taylor & Francis Group LLC, 2016. 197 p.

References

1. Savenko O.S. Research of methods of antiviral diagnostics of computer networks / O.S. Savenko, S.M. Lysenko // Herald of Khmelnytskyi National University. Technical sciences. - 2007. - № 2, v. 2. - P. 120–126.

2. Savenko O.S., Payuk V.P., Savenko B., Kashtalyan A.S. Models of undocumented software bookmarks in local computer networks. Measuring and computing equipment in technological processes. 2019. № 2. P.84-90.

3. Data Collection and Data Analysis in Honeypots and Honeynets. Pavol Sokol, Patrik Pekarčík, Tomáš Bajtoš. URL: http://spi.unob.cz/papers/2015/2015-19.pdf [Access 18.04.2020].

4. Study of Internet Threats and Attach Methods Using Honeypots and Honeynets. Tomas Sochor, Matej Zuzcak - Springer International Publishing Switzerland 2014, A. Kwiecie´n, P. Gaj, and P. Stera (Eds.): CN 2014, CCIS 431, pp. 118–127, 2014.

5. Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection. Tomas Sochor, Matey Zuzcak – Springer International Publishing Switzerland 2015, P.Gaj at al. (Eds.): CN 2015, CCIS 522, pp. 69-81, 2015. DOI: 10.1007/978-3-319-19419-6 7.

6. A Survey on Honeypot Software and Data Analysis. Marcin Nawrocki, Matthias Wählisch, Thomas C. Schmidt, Christian Keil, Jochen Schönfelder. arXiv:1608.06249v1 [cs.CR] 22 Aug 2016. URL: https://arxiv.org/abs/1608.06249 [Access 26.03.2020]

7. Composite Hybrid Techniques for Defending Against Targeted Attacks. S. Sidiroglou, A.D. Keromytis. Part of the Advanced in Information Security book series (ADIS, volume 27), 2007, 213-229 pp.

8. Shadow Honeypots. K.G. Anagnostakis, S. Sidiroglou, M. Polychronakis, A.D. Keromytis, P. Markatos. International Journal of Computer and Network Security, Vol. 2, No. 9, September 2010, 16 p.

9. POSTER: Dragging Attackers to Honeypots for Effective Analysis of Cyber Threats. Martin Husak, Jan Vykopal. URL: https://is.muni.cz/repo/1188174/POSTER-Dragging_Attackers_to_Honeypots_for_Effective_Analysis_of_Cyber_Threats.pdf [Access 30.05.2020]

10. Effective Proactive and Reactive Defense Strategies against Malicious Attacks in a Virtualized Honeynet. Frank Yeong-Sung Lin, Yu-Shun Wang, Ming-Yang Huang. Journal of Applied Mathematics, Vol. 2013, Article ID 518213, 11 pages. URL: https://www.hindawi.com/journals/jam/2013/518213/ [Access 10.04.2020]

11. A Virtual Honeypot Framework. Niels Provos. URL: http://www.citi.umich.edu/u/provos/papers/honeyd.pdf [Access 12.04.2020]

12. Securing Internet of Things (IoT) Using HoneyPots. Sai Sudha Gadde, Rama Krishna Srinivas Ganta, ASALG Gopala Gupta, Raghava Rao K, KRR Mohan Rao. International Journal of Engineering & Technology, 7 (2.7), 2018, pp. 820–824.

13. Enhancing Honeypot Deception Capability Through Network Service Fingerprinting. R.N. Dahbul, C. Lim, J. Purnama. Internation Conference on Computing and Applied Informatics 2019, Journal of Physics: Conf. Series 801. 2017.

14. Probabilistic Estimation of Honeypot Detection in Internet of Things Environment. O. Surnin, F. Hussain, R. Hussain, S. Ostrovskaya, A. Polovinkin, J.Y. Lee, X. Fernando. 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18-21 Feb. 2019, 191–196 pp.

15. Automatic Identification of Honeypot Server Using Machine Learning Techniques. Cheng Huang, Jiaxuan Han, Xing Zhang, Jiayong Liu. Hindawi, Security and Communication Networks Volume 2019, Article ID 2627608, 8 pages.

16. Survey of Attach Projection, Prediction, and Forecasting in Cyber Security. Martin Husak, Jana Komarkova, Elias Bou-Harb, Pavel Celeda. IEEE Communication Survays & Tutorials – September 2018. URL: https://www.researchgate.net/publication/327449459_Survey_of_Attack_Projection_Prediction_and_Forecasting_in_Cyber_Security [Access 12.05.2020]

17. Honeypots and Routers: Collecting Internet Attacks. Mohssen Mohammed, Habib-ur Rehman – CRC Press, Taylor & Francis Group LLC, 2016. 197 p.

Надійшла / Paper received : 04.10.2020 Надрукована/Printed :27.11.2020