DOI 10.31891/2307-5732-2020-287-4-33-38
УДК 004.75:004.8:004.49

А.С. КАШТАЛЬЯН, О.С. САВЕНКО
Хмельницький національний університет

ПОКРАЩЕННЯ БЕЗПЕКИ ТА МОДЕЛЬ АНТИВІРУСНИХ ІНТЕЛЕКТУАЛЬНИХ ПРИМАНОК В КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

В статті запропоновано модель та концепцію побудови мережі інтелектуальних приманок, розгорнутої в комп'ютерній мережі. Запропонована мережа представляє собою багаторівневу систему, що включає множину інтелектуальних приманок. Система приманок є мережею із власною архітектурою та системою сервісів, вбудована в мережу робочих сервісів, що значно підвищує контрольованість та захищеність. Мережа містить статичні та динамічні приманки із розташуванням, що забезпечує моніторинг як зовнішнього, так і внутрішнього втручання. Мережа приманок забезпечує збір, захоплення, інтелектуальний аналіз та контроль даних, раннє виявлення зловмисних дій та визначення їх характеру. Аналіз зловмисних дій, що виконує мережа приманок, передбачає пошук подібних зловмисників, пошук трендів у поведінці зловмисників, виявлення аномальної поведінки та прогнозування активності зловмисників на основі статистичних методів і методів машинного та глибокого навчання. В статті проведено аналіз відомих мереж приманок та результатів. Також визначено задачі для вирішення проблеми підвищення безпеки комп'ютерних мереж на основі використання мереж приманок.

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

A.S. KASHTALIAN, O.S. SAVENKO
Khmelnytskyi National University

SECURITY IMPROVEMENT AND THE MODEL OF ANTI-VIRUS INTELLECTUAL HONEYNET IN CORPORATE COMPUTER NETWORKS

The article proposes a model and concept of building a network of intelligent honeynet deployed in a computer network. The proposed network is a multilevel system that includes many intelligent lures. The bait system is a network with its own architecture and service system, built into the network of working services, which significantly increases controllability and security. The network contains static and dynamic lures with a location that monitors both external and internal interference. The honeynet provides data collection, capture, mining and control, early detection of malicious actions and determination of their nature. The analysis of malicious actions performed by a network of baits involves the search for similar attackers, search for trends in the behavior of attackers, detection of abnormal behavior and prediction of the activity of attackers based on statistical methods and methods of machine and deep learning. To develop honeynet focused on the use of corporate networks of enterprises (organizations) it is necessary to solve the following scientific problems: to analyze the known honeynet; analysis of methods used in baits; lure architecture; conceptual issues of building bait networks on anti-virus methods; development of a method for organizing the interaction of bait components; to formalize anti-virus baits, to allocate key features, similarly to formalize malicious software, having allocated in it the features tangent to baits which can be shown at detection; to carry out processing by the device of artificial neural networks of an event in corporate networks and dynamic change of a configuration of all honeynet, to carry out adjustment of artificial neural networks; perform experiments and process them. Solving these problems will allow you to build a honeynet that will dynamically change their configuration and have a decision-making system to respond quickly to events occurring in the network. The article analyzes the known networks of baits and results. Also, tasks have been identified to solve the problem of improving the security of computer networks based on the use of bait networks.

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

Вступ. Постановка проблеми

Під час вирішення проблем із функціонування комп'ютерних мережних ресурсів однією з найважливіших актуальних проблем є оперативне виявлення станів мережі, які призводять до часткової або повної втрати її працездатності, знищенню, спотворенню або витоку інформації, що може бути результатом зловмисних дій [1, 2]. Раннє виявлення таких станів дозволяє своєчасно усунути їх причину та уникнути наслідків.

Для виявлення зловмисних дій використовується широкий спектр систем. Проблеми захисту інформаційних ресурсів мереж вирішуються за допомогою брандмауерів (firewall), антивірусів, систем виявлення атак (Intrusion Detection System, IDS), систем контролю цілісності, криптографічних засобів захисту [3].

Використання брандмауера дозволяє контролювати проходження трафіку між локальною мережею та мережею Інтернет. Ґрунтуючись на характеристиках мережного трафіку, включаючи запитувані сервіси, джерела та визначені адреси, брандмауер приймає рішення про проходження трафіку у внутрішню мережу. Основними недоліками брандмауера є: брандмауер не може захистити від атак, які він пропускає; брандмауер не захищає від внутрішніх атак; брандмауер не може захистити від вірусу, розміщеного у файлі чи програмі.

IDS сенсори розміщують в різних місцях мережі для виявлення зловмисних подій. Робота IDS ґрунтується на пошуку попередньо визначених сигнатур зловмисних подій. Звичайно сигнатури або правила зберігаються в базах, відповідають IDS. Використання IDS також має ряд недоліків: IDS має моніторити весь мережний трафік; важко забезпечити високу швидкодію сучасних мереж із IDS; оскільки IDS моніторить весь трафік, то генерує надзвичайну кількість попереджень, що вимагає досить багато ресурсів для аналізу, крім того велика кількість цих попереджень є хибно позитивними; такі системи практично не

можуть виявити нові атаки або зловмисні дії.

Характерними особливостями цих систем є або їх періодичне та короткочасне застосування для розв'язку визначеної проблеми, або постійне використання, але зі статичними налаштуваннями. В результаті методи налізу, що здебільшого використовуються в сучасних системах, направлені на виявлення відомих та описаних втручань, але часто не можуть виявити їх модифікації або нові типи, що може зробити їх неефективними.

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. Сучасним перспективним напрямом для виявлення нових типів загроз є використання приманок в комп'ютерних мережах. Метою дослідження є підвищення достовірності процесу виявлення зловмисного програмного забезпечення в корпоративних комп'ютерних мережах на основі створення мереж приманок.

Метою роботи є проведення аналізу відомих приманок, їх елементів, виділення недоліків та визначення напрямів побудови ефективних систем виявлення зловмисних дій із залученням приманок та їх мереж.

Відомі методи виявлення приманок

Актуальні дослідження показують, що приманки, особливо об'єднані в мережі, можуть бути надзвичайно корисними для оцінки загроз у локальних мережах та мережі Інтернет. Вони виконують функції збору та аналізу інформації щодо зловмисних дій в мережах [4]. В роботах [5, 6] наведено результати використання мережі, що містить невелику низькорівневих приманок Dionaea та Kippo. Серед підходів до аналізу даних приманок переважають пряме вимірювання атак та їхнього походження. Kippo є низькорівневою приманкою, написаною на Python, що емулює SSH сервер (оболонку), містить імітацію файлової системи та можливість імітувати додавання та видалення файлів. Приманка Dionaea підтримує емуляцію доступних сервісів, включаючи SMB, http, ftp, tftp, SIP, сервери баз даних MSSQL та MySQL. Основним завданням мережі є ідентифікація атак та загроз, що надходять з мережі Інтернет, визначити найбільш вразливі місця сервісів під операційними системами Windows та Linux, з метою чого проводиться статистичний аналіз.

Крім приманок Dionaea та Kippo розроблено ряд приманок [7], серед яких низькорівневі та високорівневі, призначені для виявлення загроз сервісам з операційними системами Linux та Windows, клієнтські та серверні, реалізовані на різних мовах програмування. Існуючі приманки включають інтернет-сервіси, SMTP сервіси (приманки почтових сервісів), SSH приманки, HTTP та web приманки, телефонні приманки, безпровідні, мобільні та Bluetooth приманки, IoT приманки, ICS/SCADA приманки та спеціалізовані приманки. Також на сьогоднішній день розроблено ряд додаткових інструментів, дотичних до приманок, зокрема інструменти, що розширюють функціональність приманок та мереж та інструменти для виявлення приманок. Різноманіття приманок відображає їх універсальність у виявленні загроз у різних типах сервісів та мереж.

Окремим видом приманок є тіньові приманки, які представляють собою гібридну архітектуру, що поєднує ознаки приманок та систем виявлення втручань [8, 9]. На високому рівні використовуються різні засоби виявлення аномалій для моніторингу трафіку та захисту мережі. Трафік, який визначений цими засобами як аномальний, передається для подальшої обробки на «тіньову приманку» для подальшого уточнення його статусу. 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.

Підхід до використання приманок, який змінює їх пасивну роль очікування зловмисників на активне ефективне використання у взаємодії приманок та мережі, в якій вони розгорнуті, розглядається 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. Використовується моніторинг для визначення ранньої стадії зловмисних дій, визначення та прогнозування пізніх стадій.

Приманки використовуються у віртуальних середовищах для попередження зловмисних дій та реагування на них [10]. Віртуалізація відіграє значну роль в останніх трендах хмарних обчислень та зберігання даних, що ускладнює задачу одночасного надання якісного сервісу та захисту від втручань. Використання мережі віртуальних приманок дає можливість використовувати ефективну стратегію попередження втручань агресивних зловмисників нарівні з стратегією виявлення менш агресивних зловмисників. Віртуальні приманки та мережі віртуальних приманок розробляються також з метою зменшення витрат у порівнянні з фізичними приманками [12].

Сучасний рівень розвитку технологій дозволяє підключати до локальних мереж та мережі інтернет значний перелік різноманітних пристроїв, в тому числі це стосується інтернету речей. Підключення локальних пристроїв до таких мереж несе в собі загрозу не тільки доступу до даних, а також безпосередньо втручань в роботу цих пристроїв. Для збереження конфіденційності інформації та запобігання втручань в роботу використовуються приманки [13].

Використання приманок для захисту мереж не залишається поза увагою зловмисників. Приманки також можуть бути ідентифіковані зловмисниками з використанням різних підходів [14]. 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]. Але їх використання ускладнює процеси дослідження мережі та її вузлів зі сторони зловмисників. В залежності від потреб підвищення рівня безпеки в корпоративних комп'ютерних мережах і на виконання встановленої політики безпеки в підприємстві (організації) розгортання мереж приманок може бути ефективним рішенням для підвищення рівня безпеки. Для його реалізації потрібне вирішення проблеми комплексної побудови ефективної мережі приманок з врахування архітектури корпоративних комп'ютерних мереж та сучасних методів прийняття рішень для оперативного реагування систем захисту на комп'ютерні атаки.

Узагальнена модель приманки в корпоративних комп'ютерних мережах

Приманка встановлюється в мережі з метою бути атакованою, і не виконує інших функцій. Тому, передбачається, що на приманках немає ніякого корисного трафіку. Якщо ж на приманці фіксується будь-яка активність, то така активність вважається зловмисною [18]. Виходячи з такого визначення задач приманок і їх місця в системах захисту, можна представити узагальнену модель приманки в складі таких елементів (рис. 1) [19]:

1. Продукційна система приманки (production system, virtual production system) – власне «приманка». Вона забезпечує honey-файли та фальшиві системні ресурси для зловмисників. Система автоматично реагує на запити зловмисників з метою імітації реальної продукційної системи.

2. Брандмауер – забезпечує файли реєстрації інформації спроб зловмисника отримати доступ до приманки. Брандмауер налаштовується на запис у файл усіх активностей щодо приманки.

3. Вузол моніторингу – відслідковує, оцінює та фіксує загрози, що виникають в мережі внаслідок активності зловмисників. Аналіз порядку, послідовності, часових відміток та типів пакетів, що використовуються зловмисником для доступу до приманки, комбінації кнопок, системний доступ, зміни файлів тощо дозволяє ідентифікувати інструменти та методологію, що використовує зловмисник, а також їх наміри (несанкціонований доступ до даних, спроби віддаленого керування тощо).

4. Вузол попередження – призначений для генерування попереджень про отриманий або відправлений з приманки трафік адміністратору або системі контролю.

5. Вузол реєстрації – забезпечує ефективне зберігання для всіх файлів реєстрації трафіку між брандмауером та приманкою.

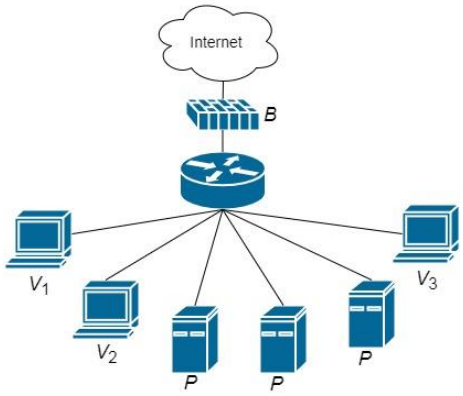

Рис. 1. Узагальнена модель приманки

Задамо узагальнену модель приманки з врахуванням її складових:

$$M = < P, B, (V_1, V_2, V_3) >, \quad (1)$$

де P – продукційна система приманки; B – брандмауер; V_1 – вузол моніторингу; V_2 – вузол попередження; V_3 – вузол реєстрації.

Робота приманки в циклі виявлення та захисту від зловмисних дій розповсюджується на етапи попередження, виявлення, реагування та дослідження зловмисних дій та атак.

Функція попередження базується на тому, що атаки передбачають пошук вразливих складових, систем та сервісів та здійснення щодо них певних несанкціонованих дій. Приманка виконується в якості такого вразливого сервісу, привабливого для зловмисників. Таким чином, часто зловмисні сервіси починають атакувати в першу чергу приманку. Захопивши активність зловмисника сервіс-приманка використовує засоби для утримання зловмисника, сповільнюючи його доступ до робочих сервісів, або в найкращому випадку запобігаючи йому. В цьому випадку використання приманки дозволяє попередити атаки щодо діючих сервісів та систем.

Функція виявлення модифікованих атак та нових типів атак приманками є критично важливою функцією для швидкого реагування та попередження втручання в мережу. На цьому етапі приманки формують невеликий та змістовний об'єм інформації про несанкціоновані дії.

Функція реагування на дії зловмисників вимагає попередньої інформації як щодо самого зловмисника, так і щодо його попередніх дій та завданої шкоди. Приманки збирають всю інформацію про атаку з самого її початку, на відміну від робочих сервісів з системами виявлення втручань. Крім того, взаємодія приманки із зловмисником може надати додаткову інформацію, яка необхідна для ефективного реагування на атаку.

Функція дослідження. Приманки є одним з найпотужніших засобів для ефективного дослідження нових видів зловмисних дій та їх модифікацій. Вся інформація, зібрана приманками, стосується тільки несанкціонованих дій, тому це є найбільш ефективний спосіб отримання такої інформації у порівнянні з іншими, наприклад з аналізом усього трафіку робочих сервісів.

Аналіз прикладу застосування приманок в комп'ютерних мережах

Застосування статистичних методів дає можливість глибоко дослідити поведінку зловмисників. Але більш затребуваними є приманки, які аналізують події динамічно і можуть приймати рішення оперативно без втручання користувача.

Розглянемо мережі приманок AWS описані в [20]. Гістограма атак по приманках відображає, яка приманка була найбільше атакована. Аналіз сервісів цієї приманки дає інформацію про найбільш привабливі сервіси для зловмисників. Приклад розподілу атак показано на рис. 2, максимальна кількість атак припадає на приманку honeypot_0003. Рис. 3 відображає геолокацію зловмисників. Статистичний аналіз дає велику кількість інформацію. Ще більше інформації можна отримати із використанням методів машинного та глибокого навчання.

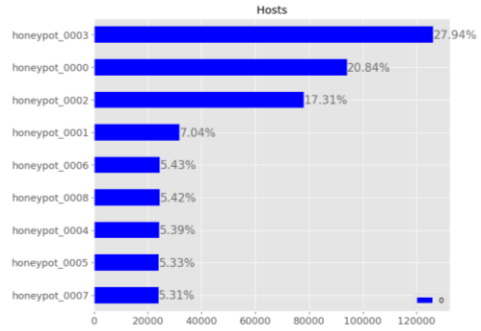

Рис. 2. Розподіл навантаження атак на приманку [20]

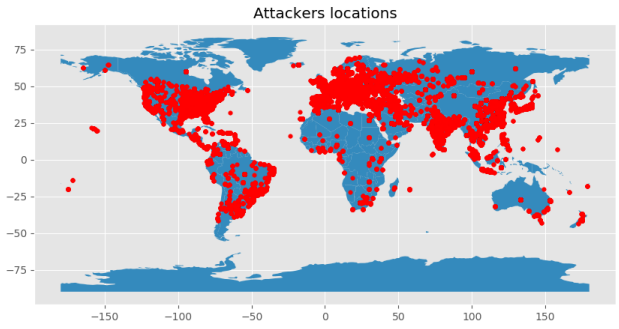

Рис. 3. Геолокація зловмисників [20]

Розглянутий приклад демонструє можливості такого засобу підвищення безпеки в комп'ютених мереж як приманки. Цей напрям дослідження є перспективним. Комплексний аналіз атак, зафіксованих мережею приманок, передбачає пошук подібних зловмисників; пошук трендів в поведінці зловмисників; аналіз викидів, які відображають підвищення активності окремих зловмисників; сумарний аналіз викидів, що відображає підвищення сумарної активності; прогнозування активності зловмисників. Проведені дослідження стосуються використання приманок у вузлах комп'ютерних мереж та окремих комп'ютерах, всі з них під'єднані до мережі Internet. Але важливою проблемою є проблема підвищення безпеки в корпоративних мережах і застосування для цього мереж приманок. Тобто вирішення цієї проблеми локально в корпоративних мережах підприємств (організацій).

Задачі для вирішення проблеми побудови мереж приманок

Для розробки мереж приманок орієнтованих на використання в корпоративних мережах підприємств (організацій) необхідно розв'язати наступні наукові задачі: провести аналіз відомих мереж приманок; аналіз методів використовуваних в приманках; архітектура приманок; концептуальні питання побудови мереж приманок на задачах антивірусних методів; розробка методу організації взаємодії компонентів приманок; формалізувати антивірусні приманки, виділити ключові особливості, аналогічно формалізувати зловмисне програмне забезпечення, виділивши в ньому дотичні для приманок особливості, які можуть проявлятись при виявленні; здійснити обробку апаратом штучних нейронних мереж події в корпоративних мережах та динамічну зміну конфігурування всієї мережі приманок, провести налаштування штучних нейронних мереж; здійснити експерименти та провести їх обробку.

Розв'язання цих задач дозволить 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 незамінним у боротьбі зі зловмисними діями, інформація про які обмежена або відсутня. Мережа інтелектуальних приманок дозволить моніторити зловмисні дії в усіх системах корпоративної комп'ютерної мережі, опрацьовувати підозрілий трафік з метою зменшення хибно позитивних спрацювань, проводити аналіз зловмисних дій на основі поточних та минулих подій, виконувати раннє виявлення маловідомих та невідомих атак, прогнозувати можливу поведінку зловмисників, оптимально використовувати ресурсі комп'ютерної мережі.

Література

1. Lysenko S. Information technology for botnets detection based on their behaviour in the corporate area network / S. Lysenko, O. Savenko, K. Bobrovnikova, A. Kryshchuk, B. Savenko // Communications in Computer and Information Science, ISSN: 1865–0929. – 2017. – Vol. 718. – P. 166–181.

2. 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.

3. 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.

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

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

6. Tomas Sochor, Matey Zuzcak. Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection. 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.

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

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

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

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

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

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

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

14. R.N. Dahbul, C. Lim, J. Purnama Enhancing Honeypot Deception Capability Through Network Service Fingerprinting. Internation Conference on Computing and Applied Informatics 2019, Journal of Physics: Conf. Series 801 (2017) 012057

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

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

17. Martin Husak, Jana Komarkova, Elias Bou-Harb, Pavel Celeda. Survey of Attach Projection, Prediction, and Forecasting in Cyber Security. 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]

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

19. R.C. Joshi, Anjali Sardana Honeypots. A new Paradigm to Information Security. Science Publishers, P.O. Box 699, Enfi eld, NH 03748, USA, 2011. 323 p.

20. AWS Honeypot Database is an open-source database including information on cyber attacks/attempts, Data has 451,581 data points collected from 9:53 pm on 3 March 2013 to 5:55 am on 8 September 2013. URL: https://www.kaggle.com/casimian2000/aws-honeypot-attack-data [Access 20.04.2020].

References

1. Lysenko S. Information technology for botnets detection based on their behaviour in the corporate area network / S. Lysenko, O. Savenko, K. Bobrovnikova, A. Kryshchuk, B. Savenko // Communications in Computer and Information Science, ISSN: 1865–0929. – 2017. – Vol. 718. – P. 166–181.

2. Savenko O.S Research of methods of antiviral diagnostics of computer networks / O.S. Savenko, S.M. Lysenko // Herald of Khmelnytskyi National University. – 2007. – Issue 2, vol. 2. – P. 120–126.

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

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

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

6. Tomas Sochor, Matey Zuzcak. Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection. 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.

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

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

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

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

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

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

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

14. R.N. Dahbul, C. Lim, J. Purnama Enhancing Honeypot Deception Capability Through Network Service Fingerprinting. Internation Conference on Computing and Applied Informatics 2019, Journal of Physics: Conf. Series 801 (2017) 012057

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

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

17. Martin Husak, Jana Komarkova, Elias Bou-Harb, Pavel Celeda. Survey of Attach Projection, Prediction, and Forecasting in Cyber Security. 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]

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

19. R.C. Joshi, Anjali Sardana Honeypots. A new Paradigm to Information Security. Science Publishers, P.O. Box 699, Enfi eld, NH 03748, USA, 2011. 323 p.

20. AWS Honeypot Database is an open-source database including information on cyber attacks/attempts, Data has 451,581 data points collected from 9:53 pm on 3 March 2013 to 5:55 am on 8 September 2013. URL: https://www.kaggle.com/casimian2000/aws-honeypot-attack-data [Access 20.04.2020].

Рецензія/Peer review : 08.10.2020 р. Надрукована/Printed : 04.11.2020 р.