reliability, in Proceedings of the 12th International Conference on Information Technology: New Generations (ITNG 2015) (Las Vegas, Nevada, 2015), pp. 796–799.

4. Boranbayev A., Boranbayev S., Yersakhanov K., Nurusheva A., Taberkhan R. (2018) Methods of Ensuring the Reliability and Fault Tolerance of Information Systems. In: Latifi S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738. Springer, Cham.

5. Chinnaiah, M., Niranjan, N. Fault tolerant software systems using software configurations for cloud computing. J Cloud Comp 7, 3 (2018). https://doi.org/10.1186/s13677-018-0104-9.

6. Zhu X, Wang J, Guo H, Zhu D, Yang LT, Liu L (2016) Fault-tolerant scheduling for real-time scientific workflows with elastic resource provisioning in virtualized clouds. IEEE Trans Parallel Distrib Syst 27(12):3501–3517. https://doi.org/10.1109/TPDS.2016.2543731.

7. Liu J, Zhou J, Buyya R (2015) Software rejuvenation based fault tolerance scheme for cloud applications In: 2015 IEEE 8th International Conference on Cloud Computing, 1115–1118, New York. https://doi.org/10.1109/CLOUD.2015.164.

8. Liu J, Wang S, Zhou A, Kumar SAP, Yang F, Buyya R (2016) Using Proactive Fault-Tolerance Approach to Enhance Cloud Service Reliability. IEEE Trans Cloud Comput PP(99):1–1. http://dx.doi.org/10.1109/TCC.2016.2567392.

9. Nicolo P (2013) A frame work for self-healing software systems In: IEEE 35th International Conference on Software Engineering (ICSE), 1397–1400. https://doi.org/10.1109/ICSE.2013.6606726.

10. Zhao W, Wenbing Z, Melliar-Smith PM, Moser LE (2010) Fault Tolerance Middleware for Cloud Computing In: 2010 IEEE 3rd International Conference on Cloud Computing, 67–74, Miami. https://doi.org/10.1109/CLOUD.2010.26.

11. Bala A, Chana I (2012) Fault tolerance- challenges, techniques and implementation in cloud computing, ISSN (Online): 16940814. IJCSI Int J Comput Sci 9(1). www.IJCSI.org.

12. Egwutuoha IP, Chen S, Levy D, Selic B (2012) A fault tolerance framework for high performance computing in cloud, Cluster, Cloud and Grid Computing (CCGrid) In: Proceedings of the 12th IEEE/ACM international symposium. 13-16 May, 709–710. https://doi.org/10.1109/CCGrid.2012.80.

13. S. Pitcher, "New DoD Approaches on the Cyber Survivability of Weapon Systems (25 March 2019)," 25 March 2019. [Online]. Available: https://www.itea.org/wp-content/uploads/2019/03/Pitcher-Steve.pdf.

14. D. J. Bodeau, R. D. Graubart, R. M. McQuaid and J. Woodill, "Cyber Resiliency Metrics and Scoring in Practice: Use Case Methodology and Examples (MTR 180449)," The MITRE Corporation, Bedford, MA, 2018.

15. D. Fitzpatrick, D. Bodeau, R. Graubart, R. McQuaid, C. Olin and J. Woodill, "(DRAFT) Cyber Resiliency Evaluation Framework for Weapon Systems: Foundational Principles and Their Potential Effects on Adversaries," The MITRE Corporation, Bedford, MA, 2019.

16. NIST, "Initial Public Draft of NIST SSP 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems," 21 March 2018. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf.

17. Lysenko, S., Savenko, O., Kryshchuk, A., Kljots, Y. Botnet detection technique for corporate area network. In: Proc. of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, pp. 363-368 (2013).

18. Savenko, O., Lysenko, S., Nicheporuk, A., Savenko, B.: Metamorphic Viruses' Detection Technique Based on the Equivalent Functional Block Search. CEUR Workshop, Vol. 1844, pp. 555–569 (2017).

19. Savenko, O., Lysenko, S., Nicheporuk, A., Savenko, B.: Approach for the Unknown Metamorphic Virus Detection. In: 9-th IEEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. Technology and Applications, pp. 453–458 (2017).

20. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A. and Nicheporuk, A.: A technique for detection of bots which are using polymorphic code. In: 21st International Conference, CN, Springer, Brunów, Poland, pp. 265-276 (2014)

21. Kondratenko, Y., Kondratenko, N.: Soft Computing Analytic Models for Increasing Efficiency of Fuzzy Information Processing in Decision Support Systems. Chapter in book: Decision Making: Processes, Behavioral Influences and Role in Business Management, R. Hudson (Ed.), Nova Science Publishers, New York, 41-78 (2015)

22. Savenko O.S Research of methods of antiviral diagnostics of computer networks / O.S Savenko, S.M Lysenko // Visnyk of Khmelnytsky National University. Technical sciences. - 2007. - № 2, v. 2. - P. 120–126.(in Ukrainian)

23. 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.(in Ukranian)

24. Savenko O.S. Model of the process of searching for Trojan programs in a personal computer / O.S. Savenko, S.M. Lysenko // Radio electronic and computer systems. - 2008. - №7. - P.87-92. (in Ukrainian)

25. Savenko O.S., Klots Y.P., Mostoviy S.V. Research and analysis of process blocking in a computer system // Visnyk of Khmelnytsky National University. - 2007. - № 3, Volume 1.- P.248-251. (in Ukrainian)

Надійшла / Paper received: 11.03.2020 Надрукована / Paper Printed : 05.06.2020

УДК 004.75:004.8:004.49
DOI: 10.31891/2219-9365-2020-65-1-16

КАШТАЛЬЯН А. С., САВЕНКО Б. О., БЕЛЬФЕР Р. Е.
Хмельницький національний університет

МОДЕЛІ ПРИМАНОК В КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ З ВРАХУВАННЯМ ТИПІВ ЗЛОВМИСНИХ АТАК

В статті розроблені моделі приманок на основі типових комп'ютерних атак, архітектурних особливостей приманок та з врахуванням архітектури розподіленої системи з приманками. Розподілена система та її компоненти стає хибним об'єктом атак і є інтегрованою в загальну систему безпеки корпоративних мереж, що загалом сприятиме покращенню рівня безпеки. Моделі 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 проаналізовано методи системного аналізу та теорії прийняття рішень для вирішення питань застосування приманок за типами атак та організації взаємодії компонентів багаторівневої системи.

Організація експериментальних досліджень представлена на основі побудови багаторівневої системи з приманками, яка динамічно змінюватиме свою конфігурацію та матиме систему прийняття рішень для оперативного реагування на події, що протікатимуть в мережі.

В статті представлено використання приманок як перспективний напрям у здійсненні захисту комп'ютерних мереж від зловмисних втручань, інформація про які обмежена або відсутня.

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

KASHTALIAN A., SAVENKO B., BELFER R.
Khmelnytsky National University

HONEYPOTS MODELS IN CORPORATE COMPUTER NETWORKS TAKING INTO ACCOUNT TYPES OF MALICIOUS ATTACKS

The article develops honeynet models based on typical computer attacks, architectural features of baits and taking into account the architecture of a distributed system with baits. The distributed system and its components become the target of false attacks and are integrated into the overall security system of corporate networks, which will generally help to improve the level of security. Bait models are the basis for the development of fundamentally new methods for detecting malicious interference in the functioning of corporate networks. The feature is the achievement by configuring different types of lures and their integration 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 analyzes methods of system analysis and decision theory for solving problems of using baits by types of attacks and organizing the interaction of components of a multilevel system.

The organization of experimental research is based on the construction of a multilevel system with baits, which will dynamically change its configuration and will have a decision-making system for rapid response to events occurring in the network.

The article presents the use of baits as a promising direction in the protection of computer networks from malicious interference, information about which is limited or absent.

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

Вступ. Постановка проблеми. Комп'ютерні мережні ресурс, які використовуються в роботі підприємств (організацій) стали невід'ємною частиною забезпечення технологічних процесів, що протікають в них. Але комп'ютерні мережі під'єднані до мережі Internet стають об'єктами для зловмисних дій [1]-[3]. Виявлення зловмисних дій та для захисту від них використовується багато різного типу та призначення систем [4]. Використовувані системи захисту корпоративних мереж не забезпечують повного надійного захисту. Тому, актуальним напрямом дослідження є пошук більш ефективних шляхів захисту від зловмисних дій в роботі мережі та виявлення їх. Основною вимогою до таких підходів є можливість виявлення нових типів, а також впливів, розподілених у часі. Перспективним напрямом захисту комп'ютерних мереж є використання окремих приманок та мереж приманок різного типу, а також їх інтеграція з іншими системами захисту. Метою дослідження є розробка моделей приманок на основі їх архітектурних особливостей, особливостей застосування та типів атак на мережі.

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 [5]-[7]. 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 [8, 9] приведено результати використання мережі, що містить невелику кількість низькорівневих приманок, які дозволяють здійснювати пряме вимірювання атак та їх походження. Приманки описані в [9]

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. Використання тіньових приманок пропонується в [10, 11]. 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 [12].

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 [13]. Віртуальні приманки та мережі віртуальних приманок дозволяють зменшити витрати у порівнянні з фізичними приманками [14]. 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 [15]. Приманки можуть бути ідентифіковані зловмисниками з використанням різних методів [16]. Ці підходи досліджуються та моделюються з метою захисту та здійснення контрзаходів щодо виявлення приманок [17, 18].

2. Моделі приманок для виявлення зловмисних дій

Для побудови моделей приманок згрупуємо і узагальнимо їх характеристики. З цією метою враховуватимемо рівні роботи приманок з урахуванням її функцій: виявлення; аналізу; реагування; виконання.

На цих рівнях здій снюється збір інформації щодо втручань в роботу сервісу, визначається із зафіксованої активності зловмисна та визначається рівень її небезпеки для мережі, формуються правила попередження та виявлення атак. А на останньому рівні відбувається поєднуєднання двох основних функції. На етапі виявлення за відомими сигнатурами виявляються атаки мережі на основі статичних патернів. На етапі попередження ці атаки блокуються як зловмисні. Тоді модель приманки, яка враховуватиме функції з яких вона формуватиметься, задамо так:

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

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

Для виявлення атаки та визначення її типу потрібно визначити характерні ознаки певного типу атаки. Приманка повинна забезпечувати:

1). порти та сервіси, на які здійснюються атаки;

2). організацію збирання, зберігання та обробки даних мережного трафіку приманки;

3). взаємодію з мережею приманок.

Порти та сервіси, розгорнуті на приманці, залежить від типу/типів атак, які перехоплює приманка. Організація збирання та зберігання даних може бути реалізована однаково для різних типів атак.

Розглянемо типові архітектури приманок з урахуванням типових атак в корпоративних мережах.

Атака «поштова бомба» направлена на електронну поштову скриню або на поштовий сервер. Основною метою цієї атаки є навмисне запобігання поштової комунікації та зниження продуктивності роботи мережі. В залежності від інтенсивності «поштової бомби» вплив атаки може бути від незручностей у використані до повної відмови в обслуговуванні.

До типових атак «поштова бомба» можна віднести:

1). масова розсилка – цілеспрямоване відправлення великої кількості випадкового поштового трафіку на цільові електронні поштові адреси;

2) посилання на список – внесення електронних поштових адрес, визначених для атаки, в численні списки підписок, таким чином використовуючи сторонні джерела для надсилання поштового трафіку на ці цільові адреси;

3) архівна бомба – надсилання дуже великого заархівованого файлу на електронну поштову адресу, визначену для атаки;

4) вкладення – надсилання повідомлень з вкладеннями значних розмірів, що має на меті перевищення об'єму пам'яті, доступної на поштовому сервері.

Характерними ознаками атаки «поштова бомба» значний об'єм поштового трафіку. Це поштовий трафік може бути сформований у різний спосіб: одне повідомлення великого об'єму; значна кількість повідомлень невеликого об'єму, направлена на одну електронну поштову адресу; значна кількість

повідомлень невеликого об'єму, направлена на різні поштові електронні адреси, розташовані на одному сервері тощо. Зловмисний поштовий трафік може надходити від одного джерела або бути розподіленим, наприклад, у випадку атаки типу «посилання на список.

Для виявлення атаки типу «поштова бомба» необхідно розгорнути на приманці SMTP-сервіс для імітації поштового серверу (рис. 1). Дані, які фіксує приманка:

- IP-адреса/ IP-префікс джерела повідомлення;
- ім'я домена/ URL/ тип URL джерела повідомлення;
- ID користувача/ користувачів;
- об'єм повідомлення, що надсилається.

На основі цих даних проводиться аналіз активності на SMTP сервісі приманки, визначаються порогові значення об'єму повідомлення/ повідомлень та швидкості їх надходження. Порогові значення використовуються для визначення поштового трафіку як зловмисного та такого, що потребує аналізу.

Рис. 1. Приманка для атаки «поштова бомба» (mailbomb)

Атаку Neptune можна охарактеризувати як напіввідкрита TCP SYN атаку. Для успішної реалізації атаки зловмисник використовує особливості попереднього встановлення з'єднання в TCP протоколі, постійно надсилаючи велику кількість SYN пакетів (запитів на встановлення зв'язку) безпосередньо на TCP сервер. Сервер надсилає у відповідь SYN/ACK пакет і чекає на ACK пакет від клієнта, який зловмисник не надсилає, і з'єднання залишається «напіввідкритим». Оскільки TCP сервер має обмежене число з'єднань, то відбувається переповнення, і робота сервера блокується.

Для виявлення атаки Neptune на приманці повинен бути розгорнутий сервіс, який працює за TCP протоколом, наприклад HTTP та FTP сервіси (рис. 2). Дані, які фіксує приманка:

- IP-адреса/ IP-префікс джерела запиту;
- ім'я домена/ URL/ тип URL джерела запиту;
- кількість «напіввідкритих» запитів.

З кількості «напіввідкритих» запитів формується часовий ряд активності зловмисників на серверах даної приманки, оскільки у випадку розподіленої атаки запити можуть надходити з різних джерел. В результаті аналізу мережний трафік класифікується як незловмисний/ зловмисний та визначаються граничне значення кількості запитів та швидкості їх надходження.

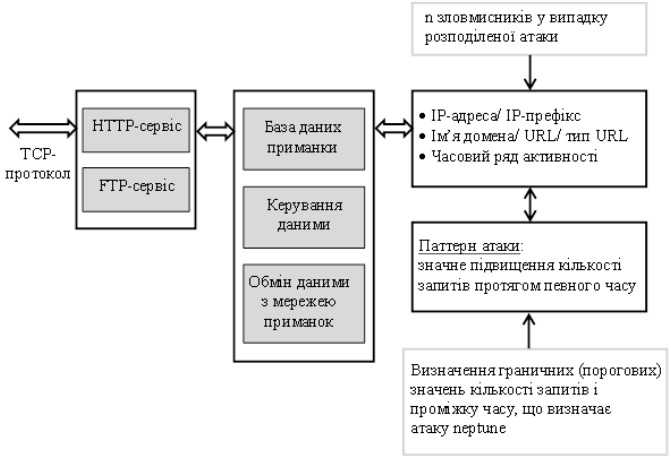

Рис. 2. Приманка для мережевої атаки neptune

Атака portsweep передбачає, що зловмисник сканує значну кількість портів цільового сервера з метою визначення сервісів, які на ньому використовуються.

Для виявлення цієї атаки на приманці має бути реалізована значна кількість портів, які можуть бути фізичні і віртуальні та відповідають портам реального сервісу. Дані, які збирає приманка:

- IP-адреса/ IP-префікс;
- ім'я домена/ URL/ тип URL;
- наявність звернення до портів.

Кількість звернень до портів формує часовий ряд активності зловмисника (зловмисників у разі розподіленої атаки). Аналіз цього ряду дає можливість класифікувати активність як зловмисну.

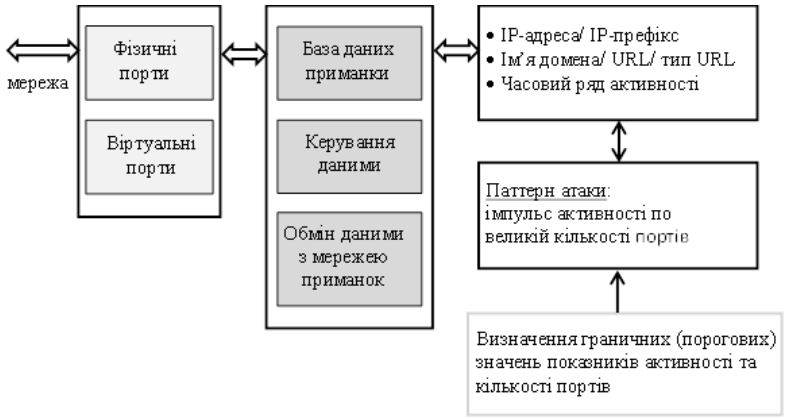

Рис. 3. Приманка для мережевої атаки portsweep

Розроблені моделі приманок для типових атак на основі (1) можуть бути застосовними для побудови мереж приманок в корпоративних мережах. Це дозволить їх використовувати в залежності від типів атак. Для організації функціонування такої мережі приманок необхідно використовувати методи теорії прийняття рішень з метою визначення динамічної зміни архітектури мережі приманок.

3. Застосування методів кластеризації поведінки зловмисників в корпоративних мережах, в яких розміщено мережу приманок для виявлення зловмисних дій

Пошук подібних зловмисників здійснюється на основі кластеризації їх поведінки, тобто часових рядів атак, які належать зловмисникам. Кластеризація часових рядів здійснюється різними методами, серед яких кластеризація на основі інформаційних критеріїв, кластеризація на основі гаусівських змішаних, кластеризація на основі прихованих марківських моделей, кластеризація на основі нейронних мереж.

Основними етапами пошуку подібних часових рядів активності зловмисників є: представлення даних ряду, вимірювання відстані між рядами, алгоритм кластеризації.

Представлення даних часового ряду має на меті виконання таких задач: значне зменшення розмірів даних, виділення основних глобальних та локальних характеристик, можливість відновлення ряду з цього представлення. Серед методів зменшення розмірності використовуються метод сингулярного спектрального аналізу, перетворення Фур'є, вейвлет-перетворення, поліноміальні перетворення, використання авто регресивного рухомого середнього тощо.

Визначення відстані між рядами, що відображає подібність, є критичним етапом для виконання подальшої кластеризації. При порівнянні поведінки зловмисників практично немає можливості застосовувати оцінки відстані, які застосовуються в класичних методах кластеризації. Необхідно застосовувати функції порівняння часових рядів, які враховують такі особливості часових рядів як можливі шуми, часові зсуви, масштабування в часі і за амплітудою, лінійні зсуви, неоднорідності та розриви. Функції порівняння часових рядів враховують подібність у часі, формі та динаміці.

Для кластеризації часових рядів активності зловмисників використовуються різні методи кластеризації, зокрема графові (алгоритм виділення зв'язаних компонент, алгоритм FOREL, функціонали якості кластеризації) , ієрархічні (агломеративні та ієрархічні алгоритми) та статистичні (EM-алгоритм, метод k-середніх), чіткі та нечіткі. У випадку чіткої кластеризації один зловмисник відноситься до одного кластеру. Аналіз активності зловмисників показує, що дії одного зловмисника можуть відноситися до декількох кластерів, тому доцільно поряд з чіткими методами кластеризації використовувати методи нечіткої кластеризації. Серед методів нечіткої кластеризації варто виділити метод c-середніх, нейромережеві (самоорганізуючі карти Кохонена тощо) та генетичні алгоритми.

Для визначення та аналізу трендів активності зловмисників здебільшого використовуються статистичні підходи, які досить широко застосовуються в економетриці. Тренд відображає загальну

тенденцію зростання, спадання або стабільність активності окремого зловмисника та групи зловмисників. Зазвичай під трендом мається на увазі глобальна довготермінова середня тенденція поведінки часового ряду. Але у випадку аналізу активності зловмисників доцільно також розглядати короткотермінові тренди в межах певного періоду, відповідно до якого приймати рішення про стан захисту мережі та подальші дії. Часовий ряд містить систематичну та несистематичну складові. В сучасних підходах до аналізу та моделювання часових рядів вважається, що часовий ряд містить три систематичних складових, рівень, тренд, періодичні коливання, та одну несистематичну, шум. Розглядаються дві моделі часових рядів, які враховують ці чотири складових: адитивна та мультиплікативна. Реальні дані можуть містити як адитивні, так і мультиплікативні складові. Для виділення тренду як однієї складової необхідно розкласти часовий ряд на складові. Одним з класичних методів є декомпозиція методом рухомого середнього, а також застосування обчислення рухомого середнього до рухомого середнього та зваженого рухомого середнього. Також, поширеним методом декомпозиції є застосування поліноміальної регресії.

Здійснення аналізу викидів в одномірних та багатомірних часових рядах дозволяє проаналізувати аномально високу та аномальну низьку активність зловмисників, це також дає інформацію про те, чи є атака розподіленою. Викиди можуть бути точковими та послідовністними. Точковим викидом є точка спостереження в певний момент часу, яка відрізняється від сусідніх точок ряду (локальний викид) або від усіх точок ряду (глобальний викид). Послідовним викидом є послідовність точок, поведінка та/або значення яких відрізняються від сусідніх точок або точок ряду, при цьому окремі точки цієї послідовності можуть не бути викидами. У випадку якщо для визначення викидів використовуються дані всього ряду, то викиди будуть глобальними, у випадку використання сусідніх точок (часового вікна) викиди будуть локальними. Особливо доцільними для аналізу атак є методи визначення викидів, які працюють з потоками даних, тому що вони дозволяють визначати, чи є дані викидами одразу після їх надходження в реальному часі.

До методів визначення точкових викидів в одномірному та багатомірному часових рядах відносяться методи, які ґрунтується на моделі, які ґрунтуються на густині та гістограмні. Найбільш популярним визначенням точкового викиду є точка, що суттєво відхиляється від очікуваного значення, визначення викиду на основі такого припущення ґрунтується на моделі часового рядку. Для побудови моделі часового ряду використовується ряд методів, серед яких вже згадані моделі рухомого середнього, декомпозиції часових рядів, штучних нейронних мереж. В процесі визначення викидів в потоках даних моделі періодично довчаються таким чином, щоб адаптуватися до надходження нових даних. Методи, що ґрунтуються на густині, визначають викиди на основі кількості сусідніх точок щодо потенційного викиду. Гістограмний метод ґрунтується на пошуку точок, видалення яких призводить до зменшення похибки гістограмного представлення часового ряду. У випадку багатомірного ряду точковий викид може стосуватися як однієї змінної ряду, так і декількох одночасно.

Для пошуку викидів в багатомірних рядах засовуються одномірні та багатомірні підходи. В одномірному підході багатомірний часовий ряд розглядається як сукупність одномірних рядів, до кожного з яких застосовується пошук викидів. Недоліком цього є не враховані кореляційні залежності багатомірного ряду, що в результаті може призвести до втрати інформації. Для уникнення цього та водночас використання одномірного підходу можуть застосовуватися методи зменшення розмірності багатомірного часового ряду. З одного боку це дозволяє зменшити кількість даних для аналізу і підвищити швидкість аналізу, з іншого боку врахувати кореляційні залежності. Серед таких методів метод головних компонент, аналіз незалежних компонент, Т-розподілене вкладення стохастичної близькості. При багатомірному підході пошук точкових викидів здійснюється із використанням одразу всіх вихідних даних без їх попереднього перетворення та розділення.

Для знаходження послідовних викидів використовуються характеристики послідовності точок одномірного або багатомірного часового ряду. До таких характеристик відносяться довжина, репрезентативність та періодичність. В більшості випадків визначаються послідовності викидів фіксованої довжини, але можливе також одночасне визначення послідовностей різної довжини. Порівняння послідовностей є більш складною задачею ніж порівняння точок, тому багато методів порівняння послідовностей для визначення викидів ґрунтуються не на оригінальних значення часового ряду, а на різних його представленнях. Зокрема з цією метою часто використовується дискретизація значень часового рядку. Періодичність послідовних викидів враховується у порівнянні з періодичністю нормальних значень часового ряду.

Прогнозування активності зловмисників передбачає раннє виявлення зловмисних дій та визначення ймовірності атак та їх характеристик на основі поточного стану та попередньо виявлених паттернів. Аналіз дій зловмисників дозволяє отримати патерни атак. Атаки можуть бути короткі та тривалі, інтенсивні та відносно непомітні. Вивчення цих патернів дозволяє вживати заходів підвищення безпеки мережі задля послаблення впливу зловмисників та зменшення втрат від втручань. Для прогнозування одномірних та багатомірних часових рядів розроблено значну кількість методів, більшість яких може бути застосована та адаптована до прогнозування різних типів атак, зокрема в мережі приманок.

До традиційних методів прогнозування часових рядів відноситься ряд методів, які ґрунтуються на авторегресії, рухомому середньому та згладжуванні. Класичні методи прогнозування часових рядів передбачають оцінку періодичності (сезонності), тренду та стаціонарності ряду, тобто передбачають певні характеристики механізму генерації значень ряду. Але в багатьох випадках, в тому числі це стосується поведінки атак, механізм генерації подій є досить складним і попередньо невідомим. В цьому випадку генеровані дані не можуть бути описані аналітичними рівняннями. В часових рядах, які описують зловмисні дії, може бути відсутній або неявний тренд. Так само період може бути відсутній або відповідати складній залежності. В цьому випадку застосування традиційних методів аналізу та прогнозування часових рядів може не привести до бажаних результатів. Натомість сучасні методи машинного та глибокого навчання не передбачають, що часовий ряд має відповідати певним характеристикам, і дозволяє прогнозувати поведінку ряду навіть якщо механізм його генерації невідомий. На сьогоднішній день розроблено ряд нейромережних методів прогнозування одномірних та багатомірних часових рядів, які ґрунтуються на використанні різних архітектур нейронних мереж, серед яких нейронні мережі прямого розповсюдження (авторегресивні нейронні мережі, авторегресивні нейронні мережі з зовнішніми входами), рекурентній нейронні мережі (нейронні мережі Елмана та Джордана, LSTM та GRU нейронні мережі), згорткові нейронні мережі. Методи глибокого навчання постійно вдосконалюються, розробляються нові механізми підвищення точності та ефективності нейронних мереж, нові комбінації архітектури (наприклад, рекурентні згорткові мережі).

4. Постановка експериментів з багаторівневою системою мережі примано

Постановку експериментів з мережею приманок в корпоративних мережах потрібно здійснювати з використанням розподіленої системи, компоненти якої мають змогу комунікувати між собою. Таку розподілену систему організовуємо так, щоб кожна її компонента була багаторівневою. Це необхідно для розміщення на різних рівнях різних модулів з приманок та різних функцій. В такій розподіленій системі передбачено рівень для організації прийняття рішеь про подальші дії. Для побудови такої розподіленої системи та розміщення в неї різного типу приманок 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. Використання приманок дозволяє створити хибні об’кти атак в комп’ютерних мережах і зібрати інформацію про атаки для аналізу, тому цей напрям досліджень є перспективним напрямом у боротьбі із зловмисними втручаннями в роботу корпоративних мереж, інформація про які обмежена або відсутня. Розроблені моделі приманок з врахуванням їх архітектурних особливостей, особливостей типових атак є основою створення системи хибних об’єктів атак, інтегровану в загальну систему безпеки корпоративних мереж, що загалом сприятиме покращенню рівня безпеки за рахунок, також, аналізу зібраної інформації в приманці про атаки. При організації виявлення та взаємодії компонентів розподіленої системи необхідним є залучення методів системного аналізу та прийняття рішень, які дозволяють покращити результат роботи всієї розроблюваної системи в цілому. Проведені дослідження таких методів дозволили виокремити важливі з них для їх застосування в розроблюваній системі. Результати експериментальних досліджень дозволяють здійснити побудову мережі приманок на основі розподіленої багаторівневої системи.

Напрямками подальших досліджень є розробка нових методів виявлення зловмисного програмного забезпечення та комп’ютерних атак і удосконалення системи підтримки прийняття рішень в багаторівневій системі, яка включає в себе приманки.

Література

1. Савенко О.С. Модель процесу пошуку троянських програм в персональному комп’ютері / О.С. Савенко, С.М. Лисенко //Радіоелектронні і комп’ютерні системи. – 2008. – №7. – С.87-92.

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. Дослідження та аналіз блокування процесів в комп'ютерній системі / О.С. Савенко, Ю.П. Кльоц, С.В. Мостовий // Вісник Хмельницького національного університету. – 2007. - № 3, Том 1.- С.248-251.

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

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

6. Sochor Tomas/ 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.

7. Sochor Tomas. 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.

8. Nawrocki Marcin/ 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 - https://arxiv.org/abs/1608.06249 [Access 26.03.2020]

9. Sidiroglou S./ 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, 213-229pp.

10. Anagnostakis K.G./ 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, 16p.

11. Husak Martin. POSTER: Dragging Attackers to Honeypots for Effective Analysis of Cyber Threats/ Martin Husak, Jan Vykopal// https://is.muni.cz/repo/1188174/POSTER-Dragging_Attackers_to_Honeypots_for_Effective_Analysis_of_Cyber_Threats.pdf [Access 30.04.2020]

12. Frank Yeong-Sung Lin/ 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 https://www.hindawi.com/journals/jam/2013/518213/ [Access 10.04.2020]

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

14. Sai Sudha Gadde/ 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.

15. Dahbul R./N. 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) 012057

16. Surnin O./ 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, 191-196pp.

17. Cheng Huang/ 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.

18. Husak Martin/ 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, https://www.researchgate.net/publication/327449459_Survey_of_Attack_Projection_Prediction_and_Forecasting_in_Cyber_Security [Access 12.05.2020]

References

1. Savenko O.S. Model of the process of searching for Trojan programs in a personal computer / O.S. Savenko, S.M. Lysenko // Radio electronic and computer systems. - 2008. - №7. - P.87-92. (in Ukrainian)

2. Savenko O.S Research of methods of antiviral diagnostics of computer networks / O.S. Savenko, S.M. Lysenko // Visnyk of Khmelnytsky National University. Technical sciences. - 2007. - № 2, v. 2. - P. 120–126. (in Ukrainian)

3. Savenko O.S., Klots Y.P, Mostoviy S.V. Research and analysis of process blocking in a computer system // Visnyk of Khmelnytsky National University. - 2007. - № 3, Volume 1.- P.248-251. (in Ukrainian)

4. 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.(in Ukranian)

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

6. Sochor Tomas/ 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.

7. Sochor Tomas. 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.

8. Nawrocki Marcin/ 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 - https://arxiv.org/abs/1608.06249 [Access 26.03.2020]

9. Sidiroglou S./ 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, 213-229pp.

10. Anagnostakis K.G./ 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, 16p.

11. Husak Martin. POSTER: Dragging Attackers to Honeypots for Effective Analysis of Cyber Threats/ Martin Husak, Jan Vykopal// https://is.muni.cz/repo/1188174/POSTER-Dragging_Attackers_to_Honeypots_for_Effective_Analysis_of_Cyber_Threats.pdf [Access 30.04.2020]

12. Frank Yeong-Sung Lin/ 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 https://www.hindawi.com/journals/jam/2013/518213/ [Access 10.04.2020]

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

14. Sai Sudha Gadde/ 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.

15. Dahbul R./N. 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) 012057

16. Surnin O./ 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, 191-196pp.

17. Cheng Huang/ 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.

18. Husak Martin/ 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, https://www.researchgate.net/publication/327449459_Survey_of_Attack_Projection_Prediction_and_Forecasting_in_Cyber_Security [Access 12.05.2020]

Надійшла / Paper received: 12.05.2020 Надрукована / Paper Printed : 04.06.2020