DOI 10.31891/2307-5732-2020-287-4-39-43
УДК 004.93

С.М. ЛИСЕНКО, Т.М. КИСІЛЬ, Ю.О. НІЧЕПОРУК, А.В. ГОРОШКО
Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ КІБЕРЗАГРОЗ ТА ШПЗ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ КОМП'ЮТЕРНИХ СИСТЕМ В КОРПОРАТИВНИХ МЕРЕЖАХ НА ОСНОВІ САМОАДАПТИВНОСТІ

В роботі представлено метод забезпечення живучості комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності, який дозволяє здійснювати адаптивне реконфігурування компонентів КС шляхом сценаріїв безпеки та забезпечує здатність системи до стійкого її функціонування в ситуації наявності кібератак. Живучість забезпечується адаптивним відновленням мережі. Ця реконструкція проводиться на основі сценарію безпеки, прийнятого на основі аналізу раніше зібраних ознак, притаманних кібератакам. Ознаки атак формуються як вектори ознак і підлягають класифікації. Результатом класифікації є віднесення об'єкту класифікації до відповідного класу, який відповідає певній кібератаці. Метою методу є вибір необхідного сценарію захисту мережевої реконструкції відповідно до кібератак. Експериментальні дослідження свідчать про високу достовірність запропонованого методу, зокрема достовірність виявлення кібератак до 99% та здатності забезпечення живучості КС в ситуації кібератак з рівнем до 70%.

Ключові слова: шкідливе програмне забезпечення, живучість, комп'ютерні системи, достовірність виявлення, кібератака, мережний трафік.

S. LYSENKO, T. KYSIL, Y. NICHEPORUK, A. GOROSHKO
Khmelnytskyi National University

METHOD FOR CYBER THREATS AND MALWARE DETECTION TO ENSURE THE COMPUTER SYSTEMS RESILIENCE OF IN CORPORATE NETWORKS BASED ON SELF-ADAPTIVITY

AThe paper presents a method for cyber threats and malware detection to ensure the computer systems resilience of in corporate networks based on self-adaptivity. The resilience is ensured by the adaptive reconfiguration of the network. Answer the question how the network has to be reconfigured is received by the means of the cluster analysis of the cyberattacks' features, which are observed in the network and network hosts. In order to choose the needed security scenarios, the proposed method uses SVM approach. The objects of classification are the feature vectors, which contain the set of the demonstrations, which may indicate the appearance of cyber threats on the in corporate networks. The purpose of the technique is to choose the network and network hosts' reconfiguration scenarios according to the cyber-attacks, performed by the botnets. The learning stage of the method consists of the following steps: a knowledge formation about the features that may indicate the cyberattacks performed by the botnet; presentation the knowledge about the cyberattacks as the set of feature vectors; a labeled data creation of the feature vectors of the cyberattacks based on knowledge. The monitoring stage of the method consists of the following steps: gathering of the inbound and outbound network traffic; gathering of the information about the hosts' network activity and reports of the hosts' antiviruses; construction of the feature vector, based on the information obtained from the network and hosts; implementation of the semi-supervised fuzzy c-means clustering for the choice of the security scenarios; implementation of the security scenarios for the corporate area network's infrastructure. Usage of the developed system makes it possible to detect known and unknown multi vector cyberattacks performed by the botnets. Experimental results demonstrated that the implemented principals of proposed technique into show the ability to ensure the resilient network functioning in the situation of the cyberattacks by botnets at the rate at about 70%.

Keywords: malware, computer systems, resilience, detection efficiency, network traffic, cyberattack.

Вступ

Сьогодні актуальною проблемою, яка призводить до негативних економічних та соціальних наслідків, є проблема боротьби із кіберзагрозами. З кожним роком результати їх впливу набирають значного масштабу, завдаючи шкоди усім сферам, де застосовуються комп'ютерні системи. Відомі методи та засоби не в змозі в повній мірі забезпечити належний рівень інформаційної безпеки. Одним з напрямків кібербезпеки, що сприяє своєчасному виявленню атак, запобіганню їх наслідків та зменшенню їх впливу є синтез живучих (резильєнтних) комп'ютерних систем – систем здатних продовжувати функціонувати в умовах здійснення кібератак [1, 2]. Тому метою роботи є підвищення достовірності виявлення атак та шкідливого програмного забезпечення (ШПЗ) з метою забезпечення живучості комп'ютерних систем в корпоративних мережах в комп'ютерних системах (КС) шляхом розроблення методу.

Пов'язані роботи

Сьогодні в наукових джерелах широко представлені різні методи виявлення кібератак в КС. Зокрема, в [3] запропоновано метод, що заснований на обробці подій для вирішення проблеми атак. У рамках цього підходу розроблено архітектуру IDS на основі моделі обробки подій (EPM). Це засновані на правилах IDS, в яких правила зберігаються в репозиторії шаблонів правил і приймають SQL і EPL Epser в якості посилання. В [4] представлено протокол аутентифікації атак КС, який використовує легкий метод шифрування, заснований на операції XOR для захисту від підробок і захисту конфіденційності. Для генерації синтезованих компонентів пропонованого полегшеного протоколу шифрування використовується САПР Quartus II. Існуючий механізм безпеки RFID-систем може бути посилений з акцентом на криптографічні протоколи. В [5] запропоновано метод виявлення Sibil атаки. Він представляє собою схему

захисту, включаючи виявлення Sibil атаки на основі соціальних графів (SGSD), а виявлення Sibil атаки на основі класифікації поведінки (BCSD). В [6] запропоновано IDS для виявлення атаки Warmhole атака за допомогою тренажера Cooja. Запропонована система використовує централізовану та розподілену архітектуру для розміщення IDS. В [7] подано технологію виявлення Sinkhole атака INTI (Intrusion Detection of Sinkhole attacks on 6LoWPAN). Інформаційна технологія INTI прагне зменшити негативний вплив атаки на КС, поєднує в собі стратегії спостереження, репутації та довіри для виявлення зловмисників шляхом аналізу поведінки пристроїв. В [8] описано інформаційну технологію радіочастотної ідентифікації в RFID – ключового протоколу шифрування, який забезпечує безпеку зв'язку, який може забезпечити аутентифікацію між міткою і сервером. В [9] описана інформаційна технологія захисту CloudEyes від атак мережного типу, яка надає ефективні та надійні служби безпеки для пристроїв з обмеженими ресурсами. CloudEyes виявляє підозрілу фільтрацію, заснована на структурі зворотних ескізів і забезпечує ретроспективне і точне наведення фрагментів злоякісної сигнатури. В [10] запропонували інформаційну технологію BMIDS (Behavioral Modeling IDS), яка використовує поведінкові шаблони. В [11] представлено нейромережний метод виявлення DDoS/DoS-атак. Виявлення було засноване на класифікації нормальних і небезпечних шаблонів. Модель ANN була перевірена на модельованій мережі Інтернету речей, що демонструє більше 99% точності. В [12] запропоновано інформаційну технологію на основі специфікації для захисту мережевої топології на основі RPL. Основна ідея полягає у вивченні станів, переходів і відповідної статистики на основі аналізу файлу трасування. Результати експериментів показують, що вище вказані методи здатні виявляти атаки, однак не забезпечують живучість КС в умовах здійснення атак.

Метод виявлення кіберзагроз та ШПЗ для забезпечення живучості комп'ютерних систем в корпоративних мережах на основі самоадаптивності

З метою реалізації принципів адаптивності та здатності до еволюції для забезпечення живучості (резильєнтності) КС в умовах кібератак розроблено метод забезпечення живучості (резильєнтності) комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності, який дозволяє здійснювати адаптивне реконфігурування компонентів КС шляхом сценаріїв безпеки та забезпечує здатність системи стійкого її функціонування в ситуації наявності кібератак [13, 14]. Живучість (резильєнтність) забезпечується адаптивною відповіддю мережі на атаку шляхом її реконфігурації, яка здійснюється на основі застосування сценарію безпеки. Висновок щодо необхідного сценарію безпеки здійснюються на основі аналізу раніше зібраних ознак, притаманних кібератакам.

Ознаки атак формуються як вектори ознак і підлягають класифікації. Результатом класифікації є віднесення об'єкту класифікації до відповідного класу, який відповідає певній кібератаці.

Метою методу є вибір необхідного сценарію захисту мережевої реконструкції відповідно до кібератак. Метод включає кроки навчання та виявлення.

1. Навчання складається з наступних етапів:

1.1. формування знань на основі особливостей, які можуть вказувати на кібератаки;

1.2. презентація знань про кібератаки як сукупність функцій векторів;

1.3. позначення отриманих векторів кібератак з метою формування класів, де кожен клас відповідає певній кібератаці, і, в свою чергу, певний сценарій безпеки, який слід застосувати для пом'якшення кібератак.

2. Етап моніторингу складається з наступних етапів:

2.1. збір вхідних та вихідних мережних даних та збір інформації про діяльність хостів мережі та звіти про антивіруси хостів;

2.2. побудова функціональних векторів на основі інформації, отриманої від мережі та хостів.

3. Етап виявлення включає в себе класифікацію множини одержаних векторів ознак на основі застосування методу опорних векторів (SVM) з метою їх віднесення до одного з класів та вибору правильного сценарію безпеки.

4. Етап відновлення включає реалізацію сценарію безпеки інфраструктури корпоративної мережі.

Позначимо набір мережних компонентів, які зазнають атак, як $B = \{b_1, b_2, b_3\}$, де b_1 – хост мережі, b_2 – мережний пристрій, b_3 – сервер у мережі, $b_i \in B$. Потім позначимо набір кібератак, як $\mathbf{A} = \{\mathbf{a}_j\}_{\mathbf{j=1}}^{\mathbf{N_A}}$. Позначимо набір сценаріїв безпеки як $S = \{s_m\}_{m=1}^{N_S}$, де N_S – кількість сценаріїв безпеки, які слід застосувати залежно від типу атаки. Таким чином, функція вибору сценарію безпеки для відновлення мережі за наявності визначеного типу атаки f може бути представлена як $f: b_i \times a_j \rightarrow s_m$. Усі ознаки є основою набору векторів $\mathbf{X} = \{\mathbf{x}_k\}_{\mathbf{k=1}}^{N}$, де кожен з вектора ознак x_k описує кібератаку, N – кількість векторів ознак. Нехай k позначає кількість попередньо визначених класів векторів ознак. Кожен клас відповідає визначеним кібератакам (і сценарій безпеки, який слід застосувати), а один клас відповідає відсутності атаки. Для здійснення класифікації множини одержаних векторів ознак в роботі застосовано метод опорних векторів (SVM) [15]. Для обчислення роздільної гіперплощини без явного проведення відображення в просторі функцій можна використовувати різні функції ядра [16]. Для проведення класифікації використовуються методи на основі «один проти всіх» та «один проти одного» SVM [17]. В роботі для здійснення класифікації векторів ознак було використано ядра: лінійне (1), поліноміальне (2), гауссове (3), експоненційне (4) та B-spline (5):

$$K(x, x_i) = x^T x_i + c, c \in R \quad (1)$$

$$K(x, x_i) = (ax^T x_i + c)^p, a \in R, c \in R, p \in N \quad (2)$$

$$K(x, x_i) = e^{\frac{\mathbf{1}}{2\sigma^2 \left\|x - x_i\right\|^2}}, \sigma > \mathbf{0} \quad (3)$$

$$K(x, x_i) = e^{\frac{\mathbf{1}}{2\sigma^2 \left\|x - x_i\right\|^2}} \quad (4)$$

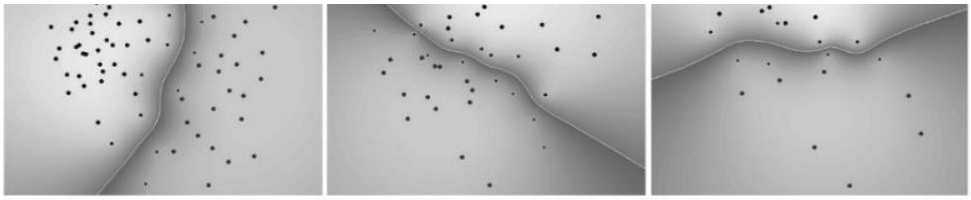
$$K(x, x_i) = B_{2p+1}(x - x_i), where\ p \in N\ with\ B_{i+1} \coloneqq B_i \otimes B_0 \quad (5)$$

З метою виявлення кібератак мережного типу проводиться моніторинг активності мережі, що може свідчити про появу кібератаки. З метою виявлення кібератаки типу хазяїна збирається інформація про мережеву діяльність хостів та звіти про антивіруси хостів. Зібрану інформацію надсилають класифікатору для подальшого аналізу. Далі, зібрані на попередньому етапі, потім аналізуються. Результатом аналізу є висновок про наявність або відсутність атаки та відповідний сценарій безпеки для відновлення мережі. В якості засобу вибору сценарію безпеки використовується SVM. На етапі виявлення об'єктами класифікації є вектори ознак x_k, отримані при аналізі корисного вхідного та вихідного трафіку. Результатом класифікації віднесення об'єкту класифікації до певного, який свідчить про необхідність застосування відповідного сценарію безпеки.

Виходячи з вибору, зробленого на попередньому етапі, слід застосувати сценарій безпеки. Кожен сценарій містить перелік дій з відновлення мережі.

Експериментальні дослідження ефективності роботи методу

Для того, щоб дослідити ефективність роботи методу, було використано різні функції ядра SVM. Приклад результатів класифікації за допомогою експоненційного ядра представлений на рис. 1. Процес класифікації поділяється на кілька ітерацій. У першій ітерації об'єкти класифікації поділяються на два класи: шкідливий і нешкідливий. Потім класифікатори поділяють об'єкти на інші два класи, наприклад: шкідливий трафік та spoofing трафік. Наступні ітерації розділяють шкідливий трафік та інші класи атак тощо, поки всі вони повністю не розділяться. Експериментальні результати різних класифікаторів SVM з'ясовували, що лінійні та поліноміальні ядра показали найгірші результати. Вони характеризувалися більш тривалими термінами виконання та вищими показниками загальної точності класифікації. Нелінійні класи класифікували кращі результати, де B-spline давав кращі результати, ніж інші. Таким чином, для експериментальних зразків оцінювання найефективнішим класифікатором, що використовує SVM, був B-spline, оскільки він забезпечував найбільшу відстань між гіперплощинами, найкоротший час оцінки та найкращу точність класифікації; таким чином, він був використаний як основна функція ядра в методі для прийняття рішення щодо застосування сценарію безпеки в залежності від класифікованої атаки.



a) b) c)

Рис. 1. Результати класифікації SVM за допомогою різних експоненційного ядра:
a) шкідливий трафік / не шкідливий трафік; b) шкідливий трафік / spoofing трафік; c) шкідливий трафік / smurf трафік

Для визначення достовірності запропонованим методом було проведено ряд експериментів. В експериментах було використано локальну мережу з 50 хостів (кожен з операційною системою Microsoft Windows), один виділений сервер (операційна система Linux OpenSusE з nginx HTTP-сервером). Експерименти тривали 24 години. Мережевий трафік захоплювався за допомогою утиліти tcpdump. Під час експериментів було здійснено 150 атак різних типів на хости, сервер та маршрутизатори. Метою було визначити, чи зможе корпоративна мережа функціонувати в ситуації атак (наприклад, якщо сервер, хости або мережний маршрутизатор зможуть надавати послуги з певними допустити характеристиками у визначений час). Як приклад, в даному підрозділі описано детальні результати експериментів із повільними DDoS, smurf та macflooding атаками [18–20]. Рис. 2 демонструє рівень мережного трафіку та часу відповіді сервера перед атакою, під час атаки та після застосування сценарію безпеки. Таким чином, видно, що під час атаки рівень трафіку залишається майже незмінним (рис. 2а), але час реакції сервера збільшувався, що спричиняло недоступність послуги (рис. 2б).

Застосування сценарію безпеки, отриманого за допомогою методу забезпечення живучості (резильєнтності) комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності виявило незначно помітні зміни рівні трафіку, в той час як час відповіді сервера зменшився і сервер зміг надавати послуги. Під час smurf атаки значно сильно збільшувались рівень трафіку та час відповіді сервера. Застосування сценарію безпеки виявила значні зменшення рівня трафіку (рис. 2а), в той час як час відповіді сервера зменшився до нормального рівня і сервер також міг функціонувати (рис. 2б).

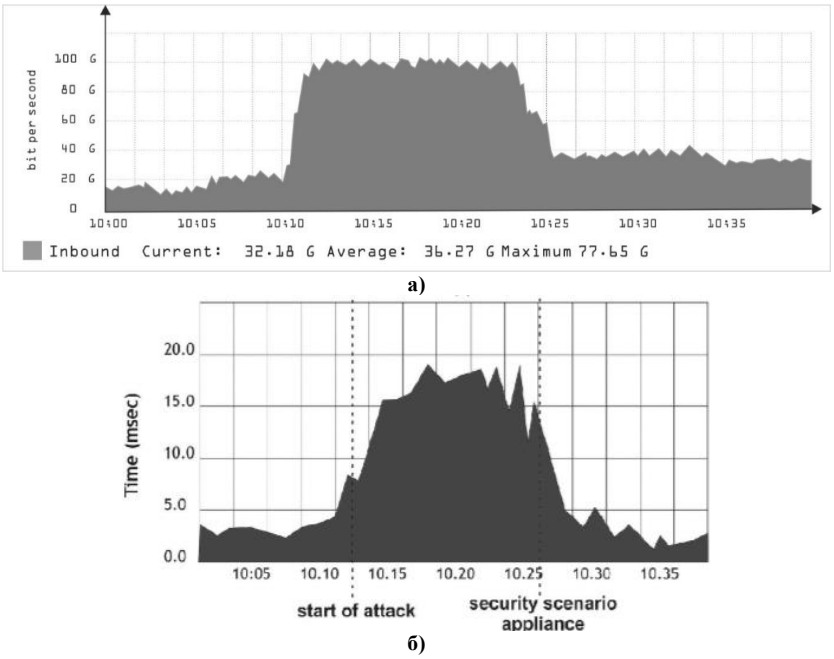


Рис. 2. Рівень трафіку (а) та часи відповіді сервера (б) до, під час та після smurf атаки

Результати показали на здатність забезпечення живучості КС в ситуації кібератак з рівнем до 70%, і продемонстрували, що метод досягає найкращих результатів для виявлення таких атак, як DDoS, ping-flooding, smurf, TCP SYN Flood, ping sweep, phishing тощо. У той же час, достовірність методу щодо Ampliation DNS, скидання TCP, RUDY, зашифровані SSL DDoS, XSS та DNS-атаки атаки нижча. Це пояснюється тим, що поведінка деяких атак дуже схожа на дії користувачів, а деякі функції атак не враховувались у процесі виявлення. Експериментальні дослідження продемонстрували високу достовірність виявлення атак запропонованим методом до 99%.

Висновки

У роботі представлено метод забезпечення живучості комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності, який, дозволяє здійснювати адаптивне реконфігурування компонентів КС шляхом сценаріїв безпеки та забезпечує здатність системи до стійкого її функціонування в ситуації наявності кібератак. Живучість забезпечується адаптивним відновленням мережі. Ця реконструкція проводиться на основі сценарію безпеки, прийнятого на основі аналізу раніше зібраних ознак, притаманних кібератакам. Ознаки атак формуються як вектори ознак і підлягають класифікації. Результатом класифікації є віднесення об'єкту класифікації до відповідного класу, який відповідає певній кібератаці. Метою методу є вибір необхідного сценарію захисту мережевої реконструкції відповідно до кібератак. Експериментальні дослідження свідчать про високу достовірність запропонованого методу, зокрема достовірність виявлення кібератак до 99% та здатності забезпечення живучості КС в ситуації кібератак з рівнем до 70%.

Література

1. McAfee Mobile Threat Report Q1, 2020. URL: https://www.mcafee.com/content/dam/cons umer/en-us/docs/2020-Mobile-Threat-Report.pdf. – 9.12.2019p. (date of access: 10.07.2020).

2. 2020 State of Malware Report. URL: https://resources.malwarebytes.com/files/2020/0 2/2020_State-of-Malware-Report.pdf (date of access: 10.07.2020).

3. Jun C., Chi C. Design of complex event-processing IDS in internet of things. In Sixth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA) (January 2014). 2014. P. 226–229.

4. Lee P. A., Clark L., Bushnell R., Poovendran A passivity framework for modeling and mitigating wormhole attacks on networked control systems, IEEE Trans. Autom. Control. 2014. Vol. 59. No. 12. Pp. 3224–3237.

5. Zhang J., Blum R.S., Lu X., Conus D. Asymptotically optimum distributed es- timation in the presence of attacks, IEEE Trans. Signal Process. 2015. Vol. 63. No. 5. P. 1086–1101.

6. Pongle P., Chavan G. Real time intrusion and wormhole attack detection in internet of things. International Journal of Computers and Applications. 2015. Vol. 121. No. 9.

7. Cervantes C., Poplade D., Nogueira M., Santos A. Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In IFIP/IEEE International Symposium on Integrated Network Management (IM)(May, 2015). 2015. P. 606–611.

8. An R., Feng H., Liu Q., Li L. Three elliptic curve cryptography-based RFID authentication protocols for Internet of Things. In International Conference on Broadband and Wireless Computing, Communication and Applications. Springer International Publishing (November 2016). 2016. P. 857–878.

9. Sun H., Wang X., Buyya R., Su J. CloudEyes: Cloud ‐ based malware detection with reversible sketch for resource ‐ constrained internet of things (IoT) devices. Software, Practice & Experience. 2017. Vol. 47. No. 3. P. 421–441. doi:10.1002/spe.2420

10. Arrington B., Barnett L., Rufus R., Esterline A. Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms. In 25th International Conference on Computer Communication and Networks (ICCCN) (August 2016). 2016. P. 1–6.

11. Hodo E., Bellekens X., Hamilton A., Dubouilh P.L., Iorkyase E., Tachtatzis C., Atkinson R. Threat

analysis of iot networks using artificial neural network intrusion detection system. In International Symposium on Networks, Computers and Communications (ISNCC)(May 2016). 2016. P. 1–6.

12. Le A., Loo J., Chai K. K., Aiash M.A. Specification-Based IDS for Detecting Attacks on RPL- Based Network Topology. Information. 2016. Vol. 7. No. 2. p. 25. doi:10.3390/info7020025

13. Lysenko S., Bobrovnikova K., Savenko O., Kryshchuk A. BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks. Communications in Computer and Information Science, ISSN: 1865-0929. 2019. P. 127–143.

14. Lysenko S., Savenko O., Bobrovnikova K., Kryshchuk A. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks. Communications in Computer and Information Science, ISSN: 1865-0929. 2018. P. 385–401.

15. Weston J., Mukherjee S., Chapelle O., Pontil M., Poggio T. Vapnik Feature selection for SVMs. In: Advances in neural information processing systems. 2001. P. 668–674.

16. Hofmann T., Scholkopf B., Smola A. J. Kernel methods in machine learning. The annals of statistics. 2008. P. 1171–1220.

17. Foody G.M., Mathur A. A relative evaluation of multiclass image classification by support vector machines. IEEE Transactions on geoscience and remote sensing. 2004. Vol. 42. No. 6. P. 1335–1343.

18. Sergii Lysenko, Pomorova Oksana, Savenko Oleg, Kryshchuk Andrii, Bobrovnikova Kira. DNS-based Anti-evasion Technique for Botnets Detection. The IEEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications: Proceedings (Warsaw, Poland, September 24-26, 2015). Warsaw, 2015. Vol. 1. P. 453–458.

19. Лисенко С.М. Методи виявлення бот-мереж в комп'ютерних системах / С.М. Лисенко, К.Ю. Бобровнікова, В.С. Харченко // Сучасні інформаційні системи. – 2019. – Т. 3. № 4. – С. 87–95.

20. Canadian Institute for Cybersecurity. Botnet dataset. URL: https://www.unb.ca/cic/datasets/botnet.html (date of access: 10.07.2020).

References

1. McAfee Mobile Threat Report Q1, 2020. URL: https://www.mcafee.com/content/dam/cons umer/en-us/docs/2020-Mobile-Threat-Report.pdf. – 9.12.2019p. (date of access: 10.07.2020).

2. 2020 State of Malware Report. URL: https://resources.malwarebytes.com/files/2020/0 2/2020_State-of-Malware-Report.pdf (date of access: 10.07.2020).

3. Jun C., Chi C. Design of complex event-processing IDS in internet of things. In Sixth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA) (January 2014). 2014. P. 226–229.

4. Lee P. A., Clark L., Bushnell R., Poovendran A passivity framework for modeling and mitigating wormhole attacks on networked control systems, IEEE Trans. Autom. Control. 2014. Vol. 59. No. 12. Pp. 3224–3237.

5. Zhang J., Blum R.S., Lu X., Conus D. Asymptotically optimum distributed es- timation in the presence of attacks, IEEE Trans. Signal Process. 2015. Vol. 63. No. 5. P. 1086–1101.

6. Pongle P., Chavan G. Real time intrusion and wormhole attack detection in internet of things. International Journal of Computers and Applications. 2015. Vol. 121. No. 9.

7. Cervantes C., Poplade D., Nogueira M., Santos A. Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In IFIP/IEEE International Symposium on Integrated Network Management (IM)(May, 2015). 2015. P. 606–611.

8. An R., Feng H., Liu Q., Li L. Three elliptic curve cryptography-based RFID authentication protocols for Internet of Things. In International Conference on Broadband and Wireless Computing, Communication and Applications. Springer International Publishing (November 2016). 2016. P. 857–878.

9. Sun H., Wang X., Buyya R., Su J. CloudEyes: Cloud‐based malware detection with reversible sketch for resource‐constrained internet of things (IoT) devices. Software, Practice & Experience. 2017. Vol. 47. No. 3. P. 421–441. doi:10.1002/spe.2420

10. Arrington B., Barnett L., Rufus R., Esterline A. Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms. In 25th International Conference on Computer Communication and Networks (ICCCN) (August 2016). 2016. P. 1–6.

11. Hodo E., Bellekens X., Hamilton A., Dubouilh P.L., Iorkyase E., Tachtatzis C., Atkinson R. Threat analysis of iot networks using artificial neural network intrusion detection system. In International Symposium on Networks, Computers and Communications (ISNCC)(May 2016). 2016. P. 1–6.

12. Le A., Loo J., Chai K. K., Aiash M.A. Specification-Based IDS for Detecting Attacks on RPL- Based Network Topology. Information. 2016. Vol. 7. No. 2. p. 25. doi:10.3390/info7020025

13. Lysenko S., Bobrovnikova K., Savenko O., Kryshchuk A. BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks. Communications in Computer and Information Science, ISSN: 1865-0929. 2019. P. 127–143.

14. Lysenko S., Savenko O., Bobrovnikova K., Kryshchuk A. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks. Communications in Computer and Information Science, ISSN: 1865-0929. 2018. P. 385–401.

15. Weston J., Mukherjee S., Chapelle O., Pontil M., Poggio T. Vapnik Feature selection for SVMs. In: Advances in neural information processing systems. 2001. P. 668–674.

16. Hofmann T., Scholkopf B., Smola A. J. Kernel methods in machine learning. The annals of statistics. 2008. P. 1171–1220.

17. Foody G.M., Mathur A. A relative evaluation of multiclass image classification by support vector machines. IEEE Transactions on geoscience and remote sensing. 2004. Vol. 42. No. 6. P. 1335–1343.

18. Sergii Lysenko, Pomorova Oksana, Savenko Oleg, Kryshchuk Andrii, Bobrovnikova Kira. DNS-based Anti-evasion Technique for Botnets Detection. The IEEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications: Proceedings (Warsaw, Poland, September 24-26, 2015). Warsaw, 2015. Vol. 1. P. 453–458.

19. Lysenko S.M. Metody vyiavlennia bot-merezh v kompiuternykh systemakh / S.M. Lysenko, K.Iu. Bobrovnikova, V.S. Kharchenko // Suchasni informatsiini systemy. – 2019. – T. 3. № 4. – S. 87–95.

20. Canadian Institute for Cybersecurity. Botnet dataset. URL: https://www.unb.ca/cic/datasets/botnet.html (date of access: 10.07.2020).

Рецензія/Peer review : 17.10.2020 р. Надрукована/Printed : 04.11.2020 р.