DOI 10.31891/2307-5732-2020-289-5-89-94
УДК 004.056.5

С.М. ЛИСЕНКО, Т.М. КИСІЛЬ, Р.В. ЩУКА
Хмельницький національний університет

ПРОЕКТУВАННЯ ТА РОЗРОБЛЕННЯ ІНТЕЛЕКТУАЛЬНОГО АГЕНТА ВИЯВЛЕННЯ КІБЕРЗАГРОЗ ТА ШПЗ В КОРПОРАТИВНИХ МЕРЕЖАХ

В роботі представлено інтелектуальний агент виявлення кіберзагроз та ШПЗ в корпоративних мережах, який представляє програмну систему із можливістю виявлення відомих та невідомих кібератак, ШПЗ мережного та хостового типу, а також здатністю продукувати множину сценаріїв безпеки для забезпечення резильєнтності КС в умовах кіберзагроз. Резильєнтність мережі та хостів забезпечується їх динамічною адаптивною реконфігурацією та множиною заходів, що дозволяють функціонувати системам в умовах атак. Інтелектуальний агент виявлення кіберзагроз та ШПЗ BotGRABBER - це мультивекторна система захисту, оскільки вона поєднує аналіз як в мережі, так і в активності хостів. Комбінована інформація дозволяє не тільки виявляти кібератаки різного типу, але й автоматично застосовувати необхідний сценарій безпеки мережної реконфігурації та адаптації КС відповідно до типу виявленої кібератаки. Інтелектуальний агент забезпечує можливість виявлення відомих та невідомих кібератак, можливість виявлення ботнетів, які використовують методи ухилення від DNS (циклічне відображення IP-адреси, "домен flux", "швидкий flux" та DNS-тунелювання), здатність самостійно застосовувати сценарії безпеки для пом'якшення кібератак, забезпечення резильєнтності корпоративних мереж в умовах кібератак, забезпечення мультивекторного захисту корпоративних мереж.

Ключові слова: шкідливе програмне забезпечення, інтелектуальний агент, кіберзагроза, кібератака, комп'ютерна мережа, сценарій безпеки.

S. LYSENKO, T. KYSIL', R. SHCHUKA
Khmelnytskyi National University

DESIGN AND DEVELOPMENT OF AN INTELLECTUAL AGENT FOR DETECTION OF CYBER THREATS AND MALWARE IN CORPORATE NETWORKS

The purpose of this paper is to develop an intellectual agent for detection of cyber threats and malware in corporate networks – BotGRABBER. It provides a novel botnet detection framework with the key features given below: ability to detect the most known botnets' cyberattacks; ability to detect the botnets that use the evasion techniques (cycling of IP mapping, "domain flux", "fast flux" and DNS-tunneling); ability to self-adaptive appliance of the security scenarios for the cyberattacks mitigation, performed by botnets; assuring the corporate area networks' resilience in the presence of botnets' cyberattacks; assurance of the multi vector protection for corporate area networks. The main components of the intellectual agent are:

1. Knowledge base. Knowledge base provides the information storage concerning to the cyberattacks performed by a botnet in the network and in the hosts. Here, each cyberattack is presented as the feature vector, which consists of functional botnets' features. To increase the efficiency of the botnet detection each stage of possible botnet's life cycle functioning (infection; initial registration or connection to C&C server; performance of the malicious activity; maintenance; its functioning termination) is presented by own feature vector.

2. Knowledge acquisition unit. Taking into account the increasing of the new ways to perform the cyberattacks proposed tool is provided by ability to update the knowledge about new botnets.

3. Network monitoring unit. This unit implements the network monitoring via gathering of the inbound and outbound network traffic. Collected information is converted into the feature vectors, and is sent to the SVM-based inference engine for further data processing.

4. Host monitoring unit. This unit implements the gathering the information about the hosts' network activity and reports of the hosts' antiviruses. It also converts the collected information into the feature vectors, and sends it to the SVM-based inference engine for further data processing.

5. SVM-based inference engine. This component provides an ability to classify the feature vectors obtained from the network. The main task of the SVM-based inference engine is to range obtained feature vector in a class, which will indicate whether it is cyberattacks, performed by botnet. If the attack is observed, the security scenario according to detected attack in order to mitigate it is to be applied.

6. Network reconfiguration unit. This unit applies produced by the SVM-based inference engine the security scenario for the CAN's infrastructure.

Keywords: malware, intellectual agent, cyberattacks, cyberthreats, computer network, security scenario.

Вступ

На сьогоднішній день з стрімким поширенням комп'ютерних систем та інформаційних технологій, а також їхньої інтеграції у глобальну мережу Internet, кібератаки та шкідливе програмне забезпечення (ШПЗ) є одним із основних видів кіберзлочинності. Збитки, заподіяні ними при інфікуванні хостів мережі, можуть бути від незначного збільшення вихідного трафіку до повного порушення працездатності мережі або втрати критично важливих даних. Причиною цього є те, що комп'ютерні системи не завжди характеризуються резильєнтністю – здатністю передбачати, протистояти, відновлюватись та пристосовуватися до атак. Відомі рішення цілісного підходу до забезпечення резильєнтного функціонування КС в умовах здійснення нових і невідомих атак [1, 2]. Тому актуальною задачею є розроблення нових підходів до виявлення нових виді кіберзагроз на основі інтелектуального аналізу даних.

Пов'язані роботи

В [3] запропоновано виявлення на основі аналізу властивості асимптотичного рівнорозподіленості (AEP) для програмного семантичного аналізу для вилучення семантично відповідних шляхів, забезпечуючи можливість семантично розуміти послідовності системних викликів. UNVEIL – інформаційна технологія, побудована на базі пісочниці для виявлення ШПЗ типу ransomware. За допомогою моделей поведінки можна виявити підозрілі дії файлової системи [4]. В [5] запропоновано метод статичного аналізу для автоматичного

виявлення поведінки динамічного завантаження коду. Евристики реалізовані для пошуку викликів методів, пов'язаних із відповідними методами. MALT – це інформаційна технологія відлагодження, яка використовує режим управління системою для прозорого аналізу шкідливих програм, і здатна аналізувати та виявляти руткіти на основі гіпервізора та ядра операційної системи (ОС) [6]. TriggerScope – інформаційна технологія, заснована на методах аналізу програм для виявлення зловмисної логіки програми, яка виконується або спрацьовує за наявності механізмів логічної бомби [7]. Targetdroid – інформаційна технологія, яка може виявити цільове ШПЗ та викликати зловмисну поведінку. Стохастична модель, що викликає поведінку, розроблена на основі ланцюгів Маркова для вираження потоку керування [8]. В [9] запропоновано інформаційну технологію аналізу ШПЗ, яка використовує методику перевірки моделі для виявлення поведінки на високому рівні, наприклад, поведінки потоку інформації. Формальна поведінка визначається як нескінченна підмножина послідовності викликів бібліотек, а набір моделей поведінки з семантичним розумінням виражається за допомогою формул лінійної часової логіки (FOLTL) першого порядку. AppContext [10] – інформаційна технологія аналізу ПЗ, яка диференціює шкідливі та доброякісні форми поведінки ПЗ. AppContext отримує контексти поведінки, залежної від безпеки, та проводить статичний аналіз для визначення поведінки, залежної від безпеки.

Архітектура інтелектуального агента виявлення кіберзагроз та шпз в корпоративних мережах

Інтелектуальний агент виявлення кіберзагроз та ШПЗ в корпоративних мережах, який має назву BotGRABBER, представляє програмну систему із можливістю виявлення відомих та невідомих кібератак, ШПЗ мережного та хостового типу, а також здатністю продукувати множину сценаріїв безпеки для забезпечення резильєнтності КС в умовах кіберзагроз. Резильєнтність мережі та хостів забезпечується їх динамічною адаптивною реконфігурацією та множиною заходів, що дозволяють фунціонувати системам в умовах атак. Інтелектуальний агент виявлення кіберзагроз та ШПЗ BotGRABBER – це мультивекторна система захисту, оскільки вона поєднує аналіз як в мережі, так і в активності хостів. Комбінована інформація дозволяє не тільки виявляти кібератаки різного типу, але й автоматично застосовувати необхідний сценарій безпеки мережної реконфігурації та адаптації КС відповідно до типу виявленої кібератаки.

Інтелектуальний агент забезпечує:

a. можливість виявлення відомих та невідомих кібератак;

b. можливість виявлення ботнетів, які використовують методи ухилення від DNS (циклічне відображення IP-адреси, “домен flux”, “швидкий flux” та DNS-тунелювання);

c. здатність самостійно застосовувати сценарії безпеки для пом'якшення кібератак;

d. забезпечення резильєнтності корпоративних мереж в умовах кібератак;

e. забезпечення мультивекторного захисту корпоративних мереж.

Компоненти архітектури інтелектуального агента представлено на рис. 1.

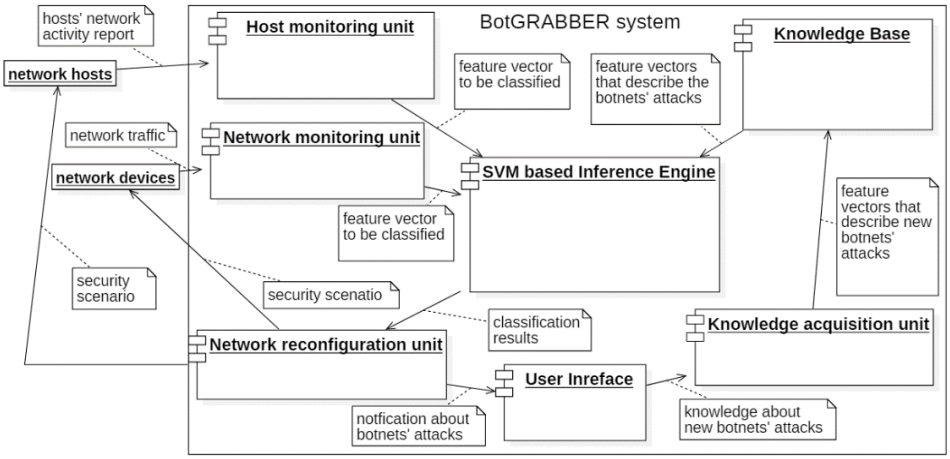

Рис. 1. Архітектура інтелектуального агента BotGRABBER

Модуль бази знань. База знань забезпечує зберігання інформації про кібератаки та шкідливе програмне забезпечення, які виконуються в мережі та на хостах. Тут кожна кібератака та ШПЗ представлені вектором ознак та дій, з яких вони складаються. Для підвищення достовірності виявлення загроз кожен етап функціонування можливого життєвого циклу атаки чи ШПЗ (зараження, початкова реєстрація або підключення до сервера C&C, виконання шкідливого функціонування, обслуговування, припинення його функціонування тощо) представлений за допомогою власного вектора ознак та дій. Перелік атак, які аналізуються системою BotGRABBER: DDoS; ping flooding; smurf attack; TCP SYN Flood; Fragmented UDP Flood; DNS Amplification; TCP Reset; ICMP Flood; RUDY; SIP INVITE Flood ; Encrypted SSL DDoS; ping sweep attack; SQL /PHP injection; Cross-Site Scripting (XSS); DNS spoofing; TCP scan/UDP scan; Phishing; Port Binding; Connect-Back; Connection Availability Abuse; Legitimate Platform Abuse; Protocol/Port Listening; Custom DNS Lookup Use; Port Reuse; Common Service Protocol/File Header Abuse.

Модуль оновлення знань. Враховуючи все більшу кількість нових способів виконання кібератак, пропонований інструмент має можливість оновити знання про нові атаки.

Модуль моніторингу мережі. Цей пристрій реалізує мережний моніторинг шляхом збору вхідної та вихідної мережі. Зібрана інформація перетворюється у функціональні вектори та надсилається до модуля висновку для подальшої обробки даних.

Модуль моніторингу хостів. Цей блок реалізує збір інформації про діяльність мережі хостів та звіти про антивіруси хостів. Він також перетворює зібрану інформацію у функціональні вектори та надсилає її до системи висновку на основі SVM для подальшої обробки даних.

Модуль здійснення висновку. Основне завдання двигуна висновку на основі SVM - присвоїти векторний елемент xi, отриманий з мережі, класу в, де $x_i \in X$, $a_t \in A$, $A = \{a_t\}_{k=1}^{N_A}$ N_A- це кількість класів , де кожному класу відповідає один заданий тип атак, виконуваних ботнетом. Двигун висновку на основі SVM робить висновок про наявність або відсутність кібератак та виявляє можливий тип атаки. Залежно від виявленого типу атаки a_t на сценарій безпеки s_q слід застосувати для відновлення мережі, $S = \{s_q\}_{q=1}^{N_S}$, де S - сукупність усіх сценаріїв безпеки, N_S - кількість захищених сценаріїв. Таким чином, функція f, вибираючи сценарій безпеки для відновлення мережі, визначається як: f: $d_u \times a_t \rightarrow s_m$, де $d_u \in D$, 1, $D = \{d_u\}_{u=1}^{N_D}$ де d_u - мережний компонент, атакований ботнетом , N_D - це кількість мережних компонентів.

Модуль відновлення. Якщо спостерігається атака, то слід застосувати сценарій безпеки, зпродукований модулем здійснення висновку, щоб пом'якшити наслідки атаки. Цей модуль застосовує сценарій безпеки. Метою сценарію безпеки є відновлення мережевої інфраструктури залежно від типу атаки.

Інтерфейсі вікна програмної реалізації інтелектуального агента виявлення кіберзагроз та шпз в корпоративних мережах представлено на рис. 2–5.

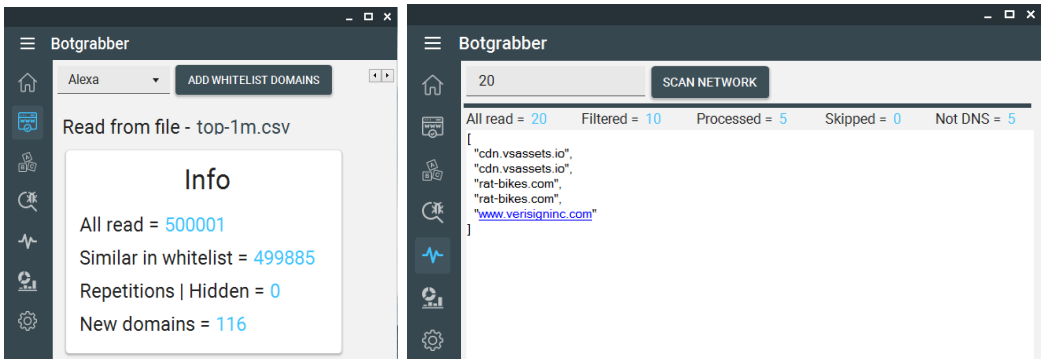

Рис. 2. Наповнення бази даних біли списків доменних імен та сканування мережі

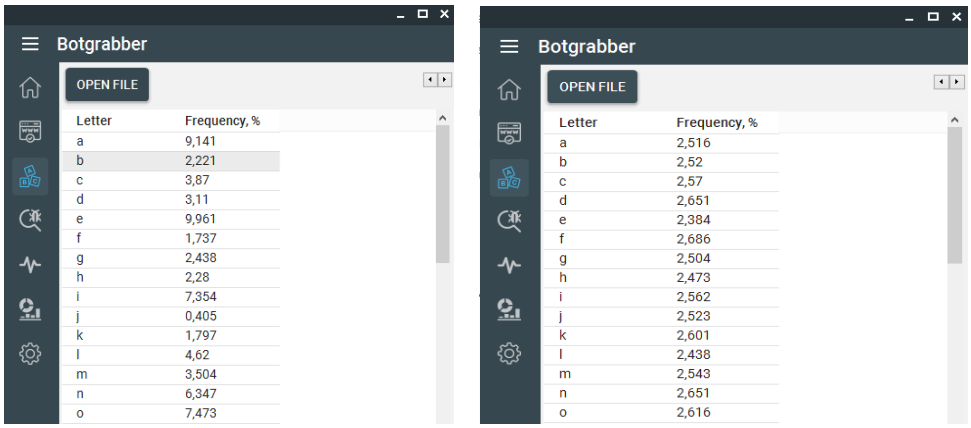

Рис. 3. Частотний лексичний аналіз відомих доменних імен та частотний лексичний аналіз доменних імен сформованих алгоритмічно

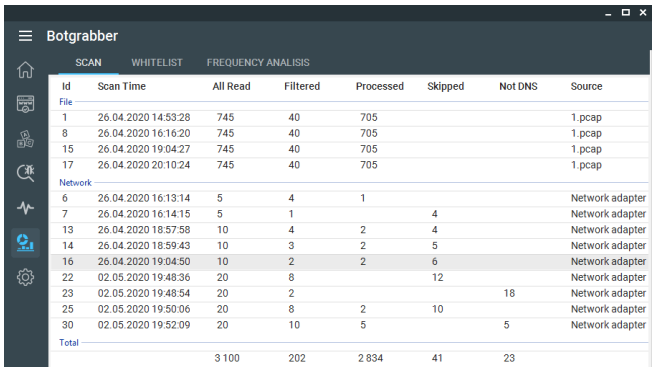

Рис. 4. Статистика сканувань мережі та файлів

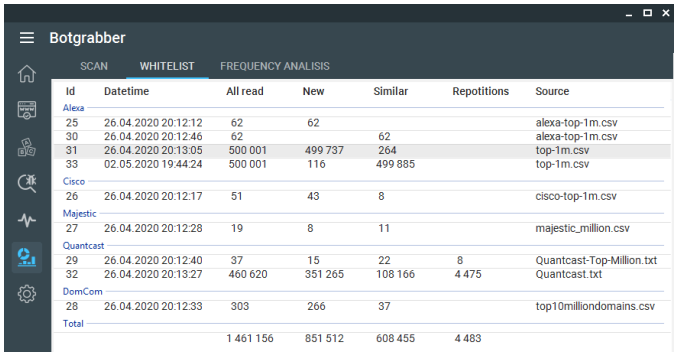

Рис. 5. Статистика наповнення бази даних білих списків доменних імен

Експерименти

Для того, щоб оцінити ефективність застосування інтелектуального агента BotGRABBER, як реалізації інформаційної технології забезпечення резильєнтності КС в умовах кіберзагроз були проведені дослідження з використанням реального мережного трафіку. Для цього було використано набір даних [11], який поєднує загальність, реалістичність та репрезентативність. Набір даних містить як шкідливі (наприклад, сліди Storm, Zeus Neris, Rbot, Virut, NSIS, Menti, Sogou, і Murlo), так і нешкідливі набори (ігрові пакети, HTTP tracc і P2P програми, такі як bittorrent). Крім того, він містить сформований реальний трафік, який імітує поведінку користувачів (наприклад, SSH, HTTP та SMTP). Набір даних поділяється на навчальні набори *T* та оцінювання (тест) E, які включають ботнетів, які виконують атаки. Набір даних включає 19755 зразків, 49,56% з яких шкідливі, а нагадування містить нормальні потоки. Тестовий набір даних включає 18917 зразків, 55,77% з яких представляють шкідливі потоки.

Для проведення експериментів, університетська локальна мережа з 50 хостів (з операційною системою Microsoft Windows), один виділений сервер (операційна система Linux OpenSusE з nginx HTTP-сервером) та мережеві пристрої (MikroTik CCR1009-8G-1S-1S + Були застосовані маршрутизатори ПК). Мережевий трафік захоплювався за допомогою утиліти tcpdump. Усі експерименти були організовані в режимі реального часу та реальних мереж і тривали від декількох секунд (наприклад, фішинг, скидання TCP, ін'єкція SQL / PHP, XSS) до однієї години (наприклад, DDoS, ping-flooding, RUDY, фрагментований UDP Flood, TCP SYN Flood тощо) залежно від типу атаки.

Для оцінювання загальної достовірність виявлення кібератак різного типу системою BotGRABBER було використано метрики, що використовуються для оцінювання якості класифікації в теорії машинного навчання [12]: чутливість, True Positive Rate (TPR) – відсоток зловмисних поведінок в КС, що класифіковані як зловмисні, $TPR = \frac{TP}{(TP+FN)}$; специфічність, True Negative Rate (TNR) – відсоток незловмисних поведінок в КС, що класифіковані як незловмисні, $TNR = \frac{TN}{(TN+FP)}$; достовірність виявлення кібератак системою BotGRABBER (Q): $Q = \frac{TP+TN}{TP+TN+FP+FN}$, де TP (true positives) – кількість шкідливих поведінок, класифікованих як шкідливі поведінки (атаки); TN (true negatives) – кількість нешкідливих поведінок, класифікованих як нешкідливі поведінки; FP (false positives) - кількість шкідливих поведінок (атак), класифікованих як нешкідливі поведінки (помилки першого роду, хибні спрацювання); FN (false negatives) - кількість класифікованих атак як нешкідливі поведінки (невиявлення, помилки другого роду).

Крім того, здатність системи BotGRABBER забезпечувати резильєнтність корпоративних мереж за наявності кібератак була оцінена за формулою: $GR = \left[R \times \frac{SRAP_{RP}}{SRAP_{DP}}\right] \times (TMPL)^{-1} \times RCAB$, де R – здатність до супротиву, яка вимірює продуктивність мережі між значеннями t_d і t_{ns}, $R \in [0,1]$, де 0 вказує на загальну втрату роботи та 1 - нормальне функціонування мережі; t_d - час, коли мережа є під впливом атаки; t_{ns} - час, коли мережу було налаштовано відповідно до сценарію безпеки, обраного системою BotGRABBER; $SRAP_{DP}$ - значення швидкості під час фази атаки; $SRAP_{RP}$ - величина швидкості під час фази відновлення мережі; *TMPL* - усереднене в часі значення втрати продуктивності мережі, яке враховує час появи атаки до відновлення мережі; *RCAB* - здатність до відновлення мережі, яка описує ефективність роботи мережі, досягнута після застосованого сценарію безпеки.

Щоб отримати кількість успішних реконфігурацій мережі, необхідно обчислити міру резильєнтності *GR*. Це безрозмірна метрика, яка дозволяє оцінити резильєнтність різних систем під різними типами атак. Таким чином, вважатимемо, що значення метрики GR, що перевищує заданий поріг *(γ> 0,7),* означає, що стабільне функціонування мережі забезпечується. Досягнення необхідного значення показника *GR* після використання сценарію захисту означає, що відновлення мережі було успішним.

Результати тестування інтелектуального агента BotGRABBER для різних класів атак представлено в таблиці 1, з якої видно, що достовірність виявлення кібератак системою BotGRABBER знаходиться в межах від 90,40% до 98,42%. Більше того, чутливість TPR та специфічність TNR знаходяться в діапазоні 91,52–99,13% та 88,46–97,52% відповідно. Тому такий підхід вказує на здатність до забезпечення резильєнтного функціонування КС в умовах кіберзагроз. Інший аспект функціонування BotGRABBER – це можливість застосовувати сценарії безпеки для кібератак за допомогою реконструкції мереж. Для того, щоб з'ясувати

можливість функціонування мережі під кібератаками, були імітовані різні типи атак на мережеві хости, сервери та доступні мережеві пристрої. Таблиця 1 демонструє, що кількість успішних реконфігурацій мережі знаходиться в діапазоні від 52,0% до 85%, середнє значення – 71,2%.

Таблиця 1

Результати тестування для різних класів атак

Тип атаки	*T*	*E*				Результат			
		Зловмисні		корисні		*SN*, %	*SP*, %	*Q*, %	*SR*, %
		TP	*FN*	*TN*	*FN*				
DDoS	574	661	16	489	14	97.64	97.22	97.46	73
Ping атака	564	585	11	465	13	98.15	97.28	97.77	76
death атака	364	568	15	429	21	97.43	95.33	96.52	76
TCP SYN	563	567	10	321	7	98.27	97.87	98.12	58
Fragmented UDP Flood	554	384	33	323	29	92.09	91.76	91.94	77
Ампліфікація DNS	421	435	38	553	41	91.97	93.10	92.60	73
Скидання TCP	671	575	31	644	19	94.88	97.13	96.06	85
ICMP attack	764	541	23	565	7	95.92	98.78	97.36	54
RUDY	198	764	36	548	39	95.50	93.36	94.59	77
SIP inv. Flood	611	434	21	561	22	95.38	96.23	95.86	79
secured SSL DDoS	571	554	41	464	35	93.11	92.99	93.05	77
Ping атака	521	494	8	198	8	98.41	96.12	97.74	69
SQL/PHP-ін'єкція	381	653	29	328	35	95.75	90.36	93.88	67
XSS	439	642	39	461	41	94.27	91.83	93.24	77
Фішинг	555	457	4	354	9	99.13	97.52	98.42	70
DNS spoofing	571	453	42	253	33	91.52	88.46	90.40	76
TCP-scan	345	451	21	326	12	95.55	96.45	95.93	67
UDP-scan	231	432	12	326	12	97.30	96.45	96.93	73
Smurf	237	344	15	433	8	95.82	98.19	97.13	68
MAC flooding	655	556	13	326	11	97.72	96.74	97.35	52

Ефективність застосування запропонованої інформаційної технології доводиться порівнянням з результатами виявлення відомими засобами виявлення атак різних типів, представленими авторитетними порталами, які розміщують аналізи останніх вірусних загроз, вивчають новітні розробки в боротьбі з вірусами та оцінки поточних антивірусних продуктів [13–15].

На рис. 6 представлено діаграму, яка демонструє результати порівняльного аналізу розробленого інтелектуального агента BotGRABBER з існуючим антивірусним програмним забезпеченням щодо найнижчих та найвищих значень достовірності виявлення атак, а також рівня резильєнтності.

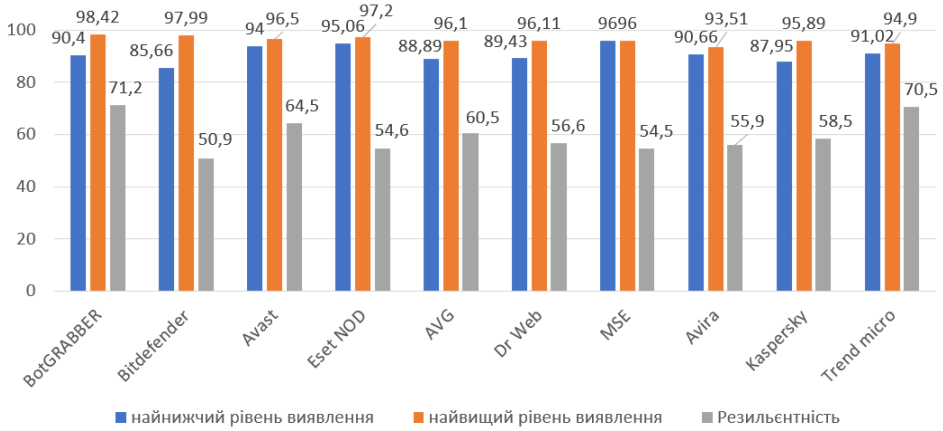

Рис. 6. Результати порівняльного аналізу інтелектуального агента BotGRABBER з існуючим антивірусним програмним забезпеченням

Висновки

Запропоновано інтелектуальний агент виявлення кіберзагроз та ШПЗ в корпоративних мережах, який представляє програмну систему із можливістю виявлення відомих та невідомих кібератак, ШПЗ мережного та хостового типу, а також здатністю продукувати множину сценаріїв безпеки для забезпечення резильєнтності КС в умовах кіберзагроз. Резильєнтність мережі та хостів забезпечується їх динамічною адаптивною реконфігурацією та множиною заходів, що дозволяють фунціонувати системам в умовах атак.

Інтелектуальний агент виявлення кіберзагроз та ШПЗ BotGRABBER – це мультивекторна система захисту, оскільки вона поєднує аналіз як в мережі, так і в активності хостів. Комбінована інформація дозволяє не тільки виявляти кібератаки різного типу, але й автоматично застосовувати необхідний сценарій безпеки мережної реконфігурації та адаптації КС відповідно до типу виявленої кібератаки.

Інтелектуальний агент забезпечує: можливість виявлення відомих та невідомих кібератак, можливість виявлення ботнетів, які використовують методи ухилення від DNS (циклічне відображення IP-адреси, "домен flux", "швидкий flux" та DNS-тунелювання), здатність самостійно застосовувати сценарії безпеки для пом'якшення кібератак, забезпечення резильєнтності корпоративних мереж в умовах кібератак, забезпечення мультивекторного захисту корпоративних мереж.

Експериментальні дослідження продемонстрували, що загальна достовірність виявлення кібератак системою BotGRABBER варіює від 90,40% до 98,42%. Більше того, чутливість та специфічність знаходяться в діапазоні 91,52–99,13% та 88,46–97,52% відповідно. Тому такий підхід вказує на здатність до забезпечення резильєнтного функціонування КС в умовах кіберзагроз.

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. – 9.12.2019. (application date: 10.07.2020).

2. 2020 State of Malware Report. URL: https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf (application date: 10.07.2020).

3. Naval S., Laxmi V., Rajarajan M., et al. Employing program semantics for malware detection. IEEE Trans Inform Forens Secur. 2015. Vol.10. No.12. P. 2591–2604. URL: https://doi.org/10.1109/TIFS.2015.2469253

4. Kharraz A., Arshad S., Mulliner C., et al. UNVEIL: a large-scale, automated approach to detecting ransomware. Proc 25th USENIX Security Symp, 2016. P. 757–772.

5. Poeplau S., Fratantonio Y., Bianchi A., et al. Execute this! Analyzing unsafe and malicious dynamic code loading in Android applications. Proc Network and Distributed System Security Symp, 2014. P. 23–26. URL: https://doi.org/10.14722/ndss.2014.23328

6. Zhang F.W., Leach K., Stavrou A., et al. Using hardware features for increased debugging transparency. Proc IEEE Symp on Security and Privacy, 2015. P .55–69. URL: https://doi.org/10.1109/SP.2015.11

7. Fratantonio Y., Bianchi A., Robertson W., et al. Triggerscope: towards detecting logic bombs in Android applications. Proc IEEE Symp on Security and Privacy, 2016. P. 377–396. URL: https://doi.org/10.1109/SP.2016.30

8. Suarez-Tangil G., Conti M., Tapiador J.E. et al. Detecting targeted smartphone malware with behavior-triggering stochastic models. Proc 19th European Symp on Research in Computer Security, 2014. P. 183–201. URL: https://doi.org/10.1007/978-3-319-11203-9_11

9. Beaucamps P., Gnaedig I., Marion J.Y. Abstraction-based malware analysis using rewriting and model checking. Proc 17th European Symp on Research in Computer Security, 2012. P. 806–823. URL: https://doi.org/10.1007/978-3-642-33167-1_46

10. Yang C., Xu Z.Y., Gu G.F., et al. DroidMiner: automated mining and characterization of fine-grained malicious behaviors in Android applications. Proc 19th European Symp on Research in Computer Security, 2014. P. 163–182. URL: https://doi.org/10.1007/978-3-319-11203-9_10.

11. Canadian Institute for Cybersecurity. Botnet dataset, (accessed January 10, 2019). URL: https://www.unb.ca/cic/datasets/botnet.html.

12. Murphy K.P. Machine learning: a probabilistic perspective. 1 st edition. The MIT press., 2012. P. 1102.

13. AV Comparatives laboratories. URL: http://www.av-comparatives.org. (application date: 26.01.2020).

14. Virus Bulletin. URL: http://www.virusbtn.com (application date: 26.01.2020).

15. Comparative antivirus testing. URL: http://www.av-comparatives.org. (application date: 26.01.2020)

Надійшла / Paper received : 05.10.2020 Надрукована/Printed :27.11.2020