УДК 004.93
DOI: 10.31891/2219-9365-2019-64-11

ЛИСЕНКО С. М.
Хмельницький національний університет

МОДЕЛІ КІБЕРАТАК МЕРЕЖНОГО ТА ХОСТОВОГО ТИПУ

В роботі представлено моделі кібератак мережного та хостового типу, які на відміну від відомих, враховують не тільки особливості їх поведінки, але й архітектурні особливості, що дозволить створити базу поведінок атак мережного та хостового типу для їх використання в процесі виявлення атак. Запропоновані принципи складають основу для розробки моделей опису здійснення кібератак на комп'ютерні системи і діляться на класи: моделі теоретико-множинного опису кібератак; моделі теоретико-множинного опису шкідливого програмного забезпечення мережного типу; моделі теоретико-множинного опису шкідливого програмного забезпечення хостового типу.

Ключові слова: кібератака, кіберзагроза, резильєнтність, комп'ютерна система, шкідливе програмне забезпечення, модель кібератаки, DoS-атака, повільна кібеатака, виявлення кібератак.

LYSENKO S.
Khmelnytskyi National University

MODELS OF THE NETWORK AND HOST CYBERATTACKS

Today cybercriminals find more ways to obtain the profit from the legitimate businesses and enterprises, which are the target of extortion and a lucrative source of income for organized crime groups because of the personally identifiable information stored and processed by these establishments. Botnets are one of the most powerful tools used by cybercriminals to commit such malicious acts. Cyberattacks are capable of spreading to any end device, including servers, routers, Network Attached Storage devices, digital video recorders, IP cameras and other smart devices. They use exploits to take over devices and enlist them with their command and control server. Antivirus software using signature-based technologies can not normally detect cyberattacks, since such new signatures are not available for newly created malware. An analysis of known methods to combat cyberattacks shows their lack of efficiency, so building a new method for detecting cyber-threats is an extremely urgent task.

The article presents models of the network and host cyberattacks which, unlike the known ones, take into account not only their behavior but also architectural features, which will allow to create a base of behavior of network and host type attacks for their use in the process of attacks detecting. The proposed principles form the basis for developing cyberattack descriptive models for computer systems and are divided into: cyberattack models of network-type malware models; host-type malware description models.

Developed models take into account components of the attacks, describes interaction between hosts, servers, firewalls of the networks and attacks, describe the set of actions of intruders including usage of Command and Control servers (C&C) describe the stages of the life cycle of the cyberattacks and the functions that are determined by the corresponding life cycle phase of cyberattack.

Keywords: cyberattack, cyberthreat, resilience, computer system, malware, cyberattack model, DoS attack, slow attack, cyberattack detection.

Вступ. Вирішальною тенденцією в галузі інформаційної безпеки корпоративних мереж є поширення кіберзагроз, до яких відносять кібератаки та шкідливе програмне забезпечення (ШПЗ). Останнім часом домінують багатовекторні кібератаки – поєднання різних типів атак в одній, що знижує ефективність їх виявлення. Найпопулярніші мультивекторні атаки поєднують, наприклад, UDP-Flood поєднувався з NTP Amplification, TCP SYN Flood та ICMP Flood [1-6].

За наявності кібератак важливим завданням є вжиття заходів, які б забезпечили послаблення (mitigate) наслідків атак та стабільне функціонування комп'ютерних систем (КС), тобто їх резильєнтність. З точки зору інформаційної безпеки резильєнтність - це здатність передбачати, протистояти, відновлюватись та пристосовуватися до несприятливих умов, зовнішніх впливів, атак чи порушення нормального функціонування системи [7-9].

Поява нових кіберзагроз, збільшення кількості шкідливих програм, а також необхідність резильєнтного функціонування мереж потребують нових інноваційних підходів для забезпечення ефективної інформаційної безпеки комп'ютерних систем у корпоративних мережах [10-14].

Поняття резильєнтності КС систем в умовах здійснення кібератак таксономічно розширюється такими принципами, на яких вона базується:

1) принцип проактивного виявлення кіберзагроз та адаптивного функціонування комп'ютерних систем в умовах здійснення кібератак;
2) принцип забезпечення стійкості до втручань в КС та забезпечення захисту в глибину;
3) принцип забезпечення диверсності компонентів КС в умовах здійснення атак;
4) принцип забезпечення еластичність та керованої деградація комп'ютерної системи;
5) принцип забезпечення здатності до еволюції КС.

Тому важливим кроком для створення резильєнтних комп'ютерних систем в умовах кіберзагроз є

розроблення множини моделей кібератак мережного та хостового типу, які на відміну від відомих, враховували б не тільки особливості їх поведінки, але й архітектурні особливості, що дозволить створити базу поведінок атак мережного та хостового типу, а також ефективних підходів до виявлення атак. Розроблені моделі можуть стати основою ефективних методів виявлення кібератак, які б забезпечили резильєнтність КС в умовах атак.

Детальне вивчення функціонування кіберзагроз та ШПЗ [15-29] дало можливість розробити моделі їх опису.

Моделі опису здійснення кіберзагроз на комп'ютерні системи

Запропоновані принципи забезпечення резильєнтності КС складають основу для розробки моделей опису кіберзагроз. Розроблені моделі діляться на класи:

1) моделі теоретико-множинного опису кібератак;
2) моделі теоретико-множинного опису шкідливого програмного забезпечення мережного типу;
3) моделі теоретико-множинного опису шкідливого програмного забезпечення хостового типу.

Розроблені моделі є інструментом опису здійснення кібератак на комп'ютерні системи та подальшого їх виявлення.

Моделі теоретико-множинного опису шкідливого програмного забезпечення мережного типу

Моделі опису здійснення кібератак на комп'ютерні системи розглядатимемо як взаємодію множини КС в комп'ютерній мережі та множини зловмисних зовнішніх впливів, які зазнають КС.

Приймемо $A=\{a_i\}_{i=1}^{N_A}$ – множина кібератак на комп'ютерні системи, N_A – кількість кібератак на КС.

Розглянемо, на приклад, кібератаки типу Port Binding у вигляді кортежу:

$$M_{a_1}=\left\langle H_{a_1},T_{a_1},D_{a_1},V_{a_1},C_{a_1},L_{a_1},F_{a_1}\right\rangle \quad (1)$$

де $H_{a_1}=\{h_i\}_{i=1}^{N_h}$ – множина КС в комп'ютерній мережі, N_h – кількість КС; $T_{a_1}=\{t_i\}_{i=1}^{N_f}$ – множина брандмауерів, присутніх в комп'ютерній мережі, N_t – кількість брандмауерів; $D_{a_1}=\{d_i\}_{i=1}^{N_d}$ множина DNS-серверів, присутніх в комп'ютерній мережі, N_d – кількість DNS-серверів; $V_{a_1}=\{v_i\}_{i=1}$ – множина дій зловмисників; $C_{a_1}=\{c_i\}_{i=1}^{N_c}$ – множина Command and Control серверів (C&C), що входять до комп'ютерної мережі, N_c – кількість C&C - серверів; $L_{a_1}=\{l_i\}_{i=1}^{4}$ – множина стадій життєвого циклу кібератаки типу Port Binding; $F_{a_1}=\{f_i\}_{i=1}^{N}f$ – множина функцій, що визначаються відповідною фазою життєвого циклу кібератаки типу Port Binding, N_f – кількість функцій; функція надсилання запиту та отримання відповіді щодо наявності брандмауера в комп'ютерній мережі з отриманням IP адреси сервера для подальшого здійснення атаки $l_1 \Rightarrow \mathrm{Y}\xrightarrow{f_1}\{t\,|t\in T\}$, де Y – множина шкідливих дій, виконуваних зловмисником, закладених в функціонал ШПЗ класу Port Binding; функція інфікування комп'ютерної системи $l_2 \Rightarrow \mathrm{Y}\xrightarrow{f_2}\{h_{\inf}\,|h_{\inf}\in H\}$, де Y – множина шкідливих дій, закладених в функціонал кібератаки типу Port Binding, H – множина КС в комп'ютерній мережі, h_{inf} – інфікована КС; функція виконання команди на здійснення шкідливої активності $l_3 \Rightarrow V\times\{p|p\in P\}\xrightarrow{f_3}\mathrm{Y}$, де P – множина команд, які можуть бути виконані в комп'ютерній мережі; функція припинення функціонування зловмисника в комп'ютерній мережі $l_4 \Rightarrow V\setminus\{v|v\in V\}\xrightarrow{f_4}V'$.

Схематичне представлення функціонування кібератаки типу Port Binding на рисунку 1.

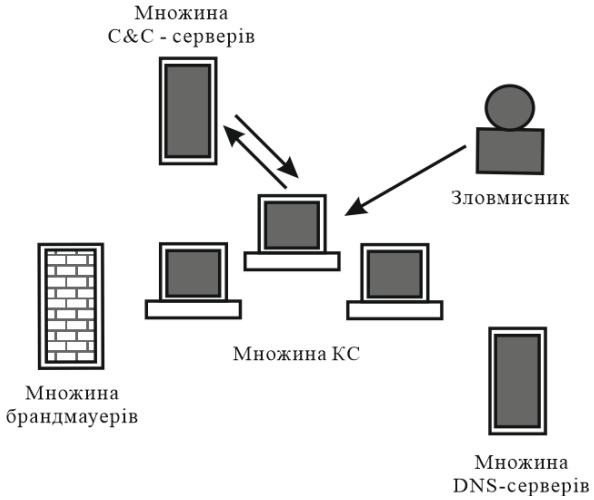

Рис. 1. Типова цільова атака на корпоративну мережу

Моделі теоретико-множинного опису шкідливого програмного забезпечення хостового типу

Представимо модель ШПЗ класу Connect-Back Technique у вигляді кортежу:

$$M_{a_2} = \left\langle H_{a_2}, T_{a_2}, V_{a_2}, C_{a_2}, \Pi_{a_2}, L_{a_2}, F_{a_2} \right\rangle \quad (2)$$

де $H_{a_2} = \{h_i\}_{i=1}^{N_h}$ – множина портів комп'ютерної системи в комп'ютерній мережі, N_h – кількість портів комп'ютерної системи; $T_{a_2} = \{t_i\}_{i=1}^{N_f}$ – множина корпоративних брандмауерів, присутніх в комп'ютерній мережі, N_t – кількість брандмауерів; $V_{a_2} = \{v_i\}_{i=1}$ – множина дій зловмисників; $C_{a_2} = \{c_i\}_{i=1}^{N_c}$ – множина Command and Control серверів (C&C), що входять до комп'ютерної мережі, N_c – кількість C&C - серверів; $\Pi_{a_2} = \{n_i\}_{i=1}$ – множин електронних листів з вкладеними зразами ШПЗ типу класу Connect-Back Technique; $L_{a_2} = \{l_i\}_{i=1}^{4}$ – множина стадій життєвого циклу ШПЗ класу Connect-Back Technique; $F_{a_2} = \{f_i\}_{i=1}^{N_f}$ – множина функцій, що визначаються відповідною фазою життєвого циклу ШПЗ класу Connect-Back Technique, N_f – кількість функцій; функція підключення систем «жертви» до Command and Control серверів (C&C) зловмисника та навпаки через порти, що не блокуються корпоративними брандмауерами для приховування своєї присутності в цільовій мережі $l_1 \Rightarrow H \xrightarrow{f_1} \{c \mid c \in C\}$, де C – множина Command and Control серверів (C&C) зловмисника; функція відправлення електронних листів до комп'ютерної системи для подальшого інфікування комп'ютерної мережі $l_2 \Rightarrow V \cup \{h_{\text{inf}} \mid h_{\text{inf}} \in H\} \xrightarrow{f_2} V'$, де V – множина шкідливих дій, закладених в функціонал ШПЗ класу Connect-Back Technique, H – множина КС в комп'ютерній мережі, h_{inf} – інфікована КС; функція використання Command and Control серверів та загальнодоступних IP – адрес для приховування своєї шкідливої активності $l_3 \Rightarrow V \xrightarrow{f_3} \{p \mid p \in P\}$, де P – множина команд, які здійснюють зв'язок з C&C серверами зловмисників в комп'ютерній мережі; функція припинення функціонування зловмисника в комп'ютерній мережі $l_4 \Rightarrow V \setminus \{v \mid v \in V\} \xrightarrow{f_4} V'$.

Схематичне представлення функціонування ШПЗ класу Connect-Back Technique на рисунку 2.

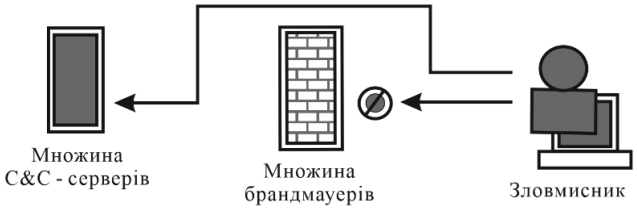

Рис. 2. Техніка зворотного зв'язку

Представимо модель ШПЗ типу Spyware у вигляді кортежу:

$$M_1 = \langle A_1, S_1, L_1, F_1, U_1, H_1, V_1 \rangle, \quad (3)$$

де $A_1 = \{a_j\}$ – множина дій користувача, що відслідковуються та збираються ШПЗ; $A_t = \{a_{t_j}\}$ - дія, що визначається даними, введеними з клавіатури (натискання клавіш); $A_s = \{a_{s_j}\}$ - дія, що визначається знімком екрану користувача комп'ютерної системи; $A_l = \{a_{l_j}\}$ - дія, що визначається отриманням списку запущених додатків у КС користувача, $A_t, A_l, A_s \in A_1$; $U_1 = \{u_j\}$ – множина дій для відслідковування дій користувача; $H_1 = \{h_j\}$ – множина дій для копіювання дій користувача, що відслідковувались; $V_1 = \{v_j\}$ – множина дій з'єднання з зловмисником, V_{em} - за допомогою електронної пошти, V_{FTP} - за допомогою FTP, V_{int} - за допомогою Інтернет, $V_{em}, V_{FTP}, V_{\text{int}} \in V_1$; S_1 – постійна пам'ять КС користувача; $L_1 = \{l_j\}_{j=1}^{6}$ – множина стадій життєвого циклу ШПЗ; $F_1 = \{f_j\}$ – множина функцій ШПЗ, що визначається відповідною фазою життєвого циклу; функція інфікування КС $l_1^1 \Rightarrow \mathrm{Y} \xrightarrow{f_1^1} \{c_{\text{in}} | c_{\text{in}} \in C\}$, де Y – множина шкідливих дій, закладених в функціонал ШПЗ, C – множина КС в мережі, c_{in} – інфікована ШПЗ КС; функція відслідковування даних користувача $l_2^1 \Rightarrow U_1 \xrightarrow{f_2^1} \{a | a \in A_1\}$; функція копіювання даних користувача, що відслідковувались $l_3^1 \Rightarrow H_1 \xrightarrow{f_3^1} \{a | a \in A_1\}$; запис зібраних даних в пам'ять КС користувача $l_4^1 \Rightarrow S_1 \cup \{a | a \in A_1\} \xrightarrow{f_4^1} S_1^{'}$; виконання команди передачі зібраних даних зловмиснику через мережу Інтернет $l_5^1 \Rightarrow V_1 \xrightarrow{f_5^1} S_1^{'}$; видалення зібраних даних користувача з системної пам'яті КС $l_6^1 \Rightarrow S_1 \setminus S_1^{'} \xrightarrow{f_6^1} S_1$.

Моделі теоретико-множинного опису кібератак

Розглянемо моделі кібератак на прикладі повільної DDoS-атаки. З цією метою позначимо атаку як A, тоді множину веб-серверів для здійснення атаки приймемо як $B = \{b_i\}_{i=1}^{N_b}$, де N_b- кількість веб-серверів;

Тоді моделі веб-серверів b_i у вигляді кортежів будуть мати такий вигляд:

$$M_{b_i} = (C_{1_{b_i}}, C_{2_{b_i}}, D_{b_i}) \quad (4)$$

де, $C_{1_{b_i}}$ – IP-адреса веб-сервера; $C_{2_{b_i}}$ – URL-адреса веб-сервера; $D_{b_i} = \{d_i\}_{i=1}^{N_d}$ – множина веб-форм для відправки даних, N_d- кількість веб-форм.

Представимо модель веб-форм d_i у вигляді кортежу:

$$M_{d_i} = (E_{d_i}) \quad (5)$$

де $E_{d_i} = \{e_i\}_{i=1}^{N_e}$ – множина параметрів веб-форми для здійснення атаки, N_e- кількість параметрів.

В такому випадку модель повільної DDoS атаки у вигляді кортежу буде мати такий вигляд:

$$M_A = (B, F_0, F_1, G_0, H_A, K_A, L_A) \quad (6)$$

де $F_0 = \{f_{0_i}\}_{i=1}^{N_{f_0}}$ – множина брандмауерів, присутніх в комп'ютерній мережі, N_{f_0} - кількість брандмауерів;

$F_1 = \{f_{1_i}\}_{i=1}^{N_{f_1}}$ – множина проксі-серверів для приховування зловмисника, N_{f_1} - кількість проксі-серверів;

$G_0 = \{G_1, G_2, G_3, G_4\}$ – множина дій зловмисника, де $G_1 = \{g_{1_i}\}_{i=1}$– множина дій зловмисника для визначення адреси веб-сервера; $G_2 = \{g_{2_i}\}_{i=1}$– множина дій зловмисника для вибору веб-форми; $G_3 = \{g_{3_i}\}_{i=1}$– множина дій зловмисника для вибору параметра веб-форми; $G_4 = \{g_{4_i}\}_{i=1}$– множина дій зловмисника для вибору кількості підключень; $H_A = \{h_i\}_{i=1}^{N_h}$ – множина POST HTTP запитів, які створює повільна DDoS атака, N_h- кількість POST HTTP запитів.

Представимо модель POST HTTP запитів h_i у вигляді кортежу:

$$M_{h_i} = (J_{0_{h_i}}) \quad (7)$$

де $J_{0_{h_i}} = \{j_{0_i}\}_{i=1}^{N_{j_0}}$ – множина IP-пакетів, які належать відповідним POST HTTP запитам., N_{j_0}- кількість IP-пакетів; $K_A = \{k_i\}_{i=1}^{6}$ – множина етапів здійснення повільної DDoS атаки; $L_A = \{l_i\}_{i=1}^{N_l}$ – множина функцій, що визначаються відповідним етапом здійснення повільної DDoS атаки, N_l- кількість функцій.

Множину етапів K_A здійснення повільної DDoS атаки можна представити у вигляді набору послідовних функцій $l_1 \ldots l_6$:

$k_1 \Rightarrow G_1 \times \{b \mid b \in B\} \xrightarrow{l_1} Y$ – функція визначення адреси веб-сервера, де Y – множина дій, виконуваних зловмисником, закладених в функціонал повільної DDoS атаки; $k_2 \Rightarrow G_2 \times \{b \mid b \in B\} \xrightarrow{l_2} Y$ – функція вибору веб-форми відповідного веб-сервера, де Y – множина дій, виконуваних зловмисником, закладених в функціонал повільної DDoS атаки; $k_3 \Rightarrow G_3 \times \{d \mid d \in D\} \xrightarrow{l_3} Y$ - функція вибору параметра відповідної веб-форми, де Y – множина дій, виконуваних зловмисником, закладених в функціонал повільної DDoS атаки; $k_4 \Rightarrow G_4 \times \{e \mid e \in E\} \xrightarrow{l_4} Y$ – функція вибору кількості підключень, які створюватиме повільна DDoS атака, де Y – множина дій, виконуваних зловмисником, закладених в функціонал повільної DDoS атаки; $k_5 \Rightarrow Y \xrightarrow{l_5} \{b \mid b \in B\}$ – функція встановлення з'єднань за допомогою надсилання POST HTTP запитів, де Y – множина дій, виконуваних зловмисником, закладених в функціонал повільної DDoS атаки; $k_6 \Rightarrow G_0 \setminus \{g_1, g_2, g_3, g_4\} \xrightarrow{l_6} G_0'$ - функція припинення функціонування зловмисника в комп'ютерній мережі.

Для надсилання даних, які генерує повільна DDoS атака, керування серверами та ідентифікації можливих об'єктів атаки зловмисники найбільш часто використовують множину стандартних портів z_i.

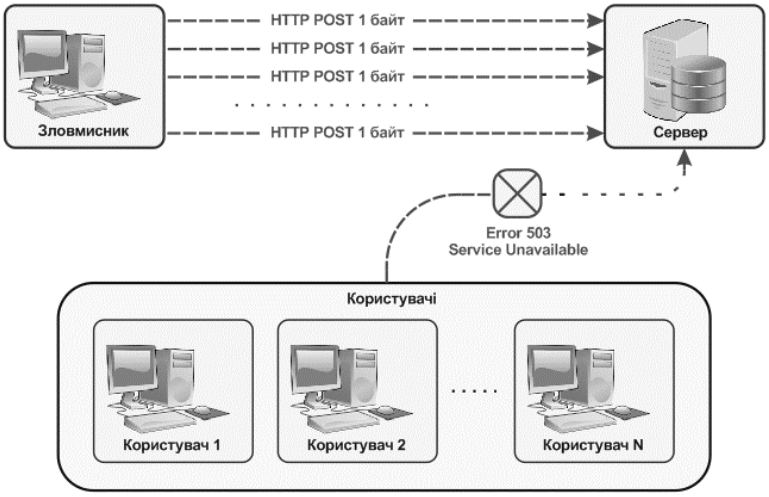

Рис. 3. Схема процесу реалізації повільної DDoS атаки

Експерименти

Для здійснення оцінки адекватності розроблених моделей було проведено ряд експериментів на прикладі залучення моделей теоретико-множинного опису кібератак. З цією метою в експериментах було використано локальну мережу з 50 хостів (кожен з операційною системою Microsoft Windows), та 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 атаки різного типу проти хостів мережі, сервера та маршрутизаторів на основі залучення множини зразків навчального набору *T*, множини зразків *E* (включаючи злісні та доброякісні зразки трафіку. Метою було з'ясувати, чи є можливим здійснення виявлення атак із залученням розроблених моделей. Як приклад в даній статті розглядаються детальні результати експериментів із атаками: R.U.D.Y., smurf та MAC flooding [23].

R.U.D.Y. атака – тип повільної DDoS атаки, призначена для здійснення відмови веб-сервера шляхом подання полів довгої форми. Атака виконується за допомогою інструменту DoS, який переглядає цільовий веб-сайт та виявляє вбудовані веб-форми. Після виявлення форм, R.U.D.Y. надсилає законні HTTP-запити POST з ненормально довгим заголовком "довжина вмісту". Такий тип атаки важко виявити порівняно з об'ємними DDoS-атаками, які помітні через аномально високого спрацьовування вхідного трафіку. Для здійснення цієї атаки R.U.D.Y. був використаний засіб імітації атаки [27].

Для smurf атаки характерна велика кількість пакетів ICMP з підробленим IP-адресою жертви в мережу з використанням IP-широкомовної адреси. Це змушує пристрої в мережі реагувати, надсилаючи відповідь на IP-адресу джерела. Для того, щоб здійснити атаку, було використано мережевий генератор пакетів Hyenae [28].

Атака macflooding має конфігураційну таблицю апаратного забезпечення для зберігання вихідних адрес усіх отриманих пакетів: коли ця таблиця стане повною, трафік, який спрямований на адреси, які вже неможливо дізнатись, буде остаточно відтворений [29].

Рис. 4 демонструє рівень мережного трафіку та часу відповіді сервера перед атакою, під час атаки та після її виявлення із застосуванням необхідних заходів безпеки. Результати експериментів (табл. 1) продемонстрували, що залучення розроблених моделі в процес проактивного виявлення атак показали його високу достовірність.

Варто зазначити, що достовірність виявлення smurf та MAC flooding атак вища, ніж RUDY, оскільки, що моделі поведінки деяких атак дуже схожа на дії користувачів, а деякі функції атак не можуть враховуватися у процесі виявлення.

Для оцінювання загальної достовірність виявлення кібератак різного типу було використано метрики: 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 $Q = \frac{TP+TN}{TP+TN+FP+FN}$, 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).

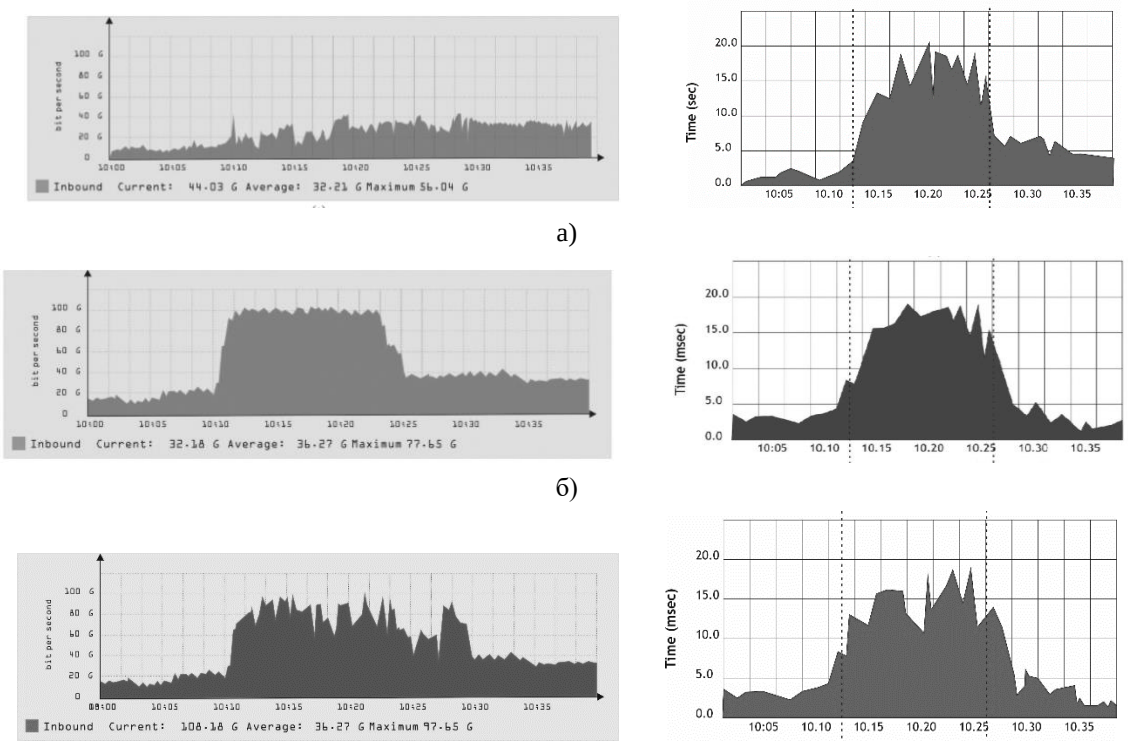

Рис.4. Рівень трафіку та час відповіді сервера до, під час та після атак: а) повільної DDoS атаки R.U.D.Y; б) smurf; в) macflooding

З таблиці 1 видно, що застосування розроблених моделей забезпечує високу достовірність виявлення кібератак і знаходиться в межах від 94,59% до 97,35%. Більше того, чутливість TPR та специфічність TNR знаходяться в діапазоні 91,52–99,13% та 88,46–97,52% відповідно.

Таблиця 1

Результати виявлення атак

Тип атаки	T	E				Результат		
		Зловмисні		корисні		*TPR*, %	*TNR*, %	Q, %
		TP	FN	TN	FN			
RUDY	198	764	36	548	39	95.50	93.36	94.59
smurf	237	344	15	433	8	95.82	98.19	97.13
MAC flooding	655	556	13	326	11	97.72	96.74	97.35

Висновки. В даній статті розроблено та описано моделі кібератак мережного та хостового типу, які на відміну від відомих, враховують б не тільки особливості їх поведінки, але й архітектурні особливості, що дозволить створити базу поведінок атак мережного та хостового типу для їх використання в процесі виявлення атак.

Запропоновані принципи складають основу для розробки моделей опису здійснення кібератак на комп'ютерні системи і діляться на класи: моделі теоретико-множинного опису кібератак; моделі теоретико-множинного опису шкідливого програмного забезпечення мережного типу; моделі теоретико-множинного опису шкідливого програмного забезпечення хостового типу.

Експериментальні дослідження продемонстрували, що практичне залучення розроблених моделі в процес проактивного виявлення атак показали його високу достовірність, яка знаходиться в межах від 94,59% до 97,35%.

References

1. NEXUSGUARD. DDoS Threat Report 2019 Q3. Available at: https://www.nexusguard.com /threat-report-q3-2019 (accessed 9.01.2020).
2. Oxford Dictionaries. Available at: http://www. oxforddictionaries.com/definition/english/botnet?q=botnet (accessed 9.01.2020).
3. Lysenko, S., Savenko, O., Kryshchuk, A., Kljots, Y. Botnet detection technique for corporate area network. In: Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013, pp. 363-368.
4. Zuzcak, M., Sochor, T. Behavioral analysis of bot activity in infected systems using honeypots. In: Communications in Computer and Information Science: Springer, Cham, 2017, vol. 718, pp. 118-133.
5. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A., Bobrovnikova, K. Antievasion technique for the botnets detection based on the passive DNS monitoring and active DNS probing. In: International Conference on Computer Networks: Springer International Publishing, 2016, pp. 83-95.
6. Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A., Savenko, B. Information Technology for Botnets Detection Based on Their Behaviour in the Corporate Area Network. In: International Conference on Computer Networks: Springer, Cham, 2017, pp. 166-181.
7. SearchDataCenter. Data center resiliency. Available at: http://searchdatacenter.techtarget. com/definition/resiliency (accessed 9.01.2020).
8. Bodeau, D., Graubart, R. Structured Cyber Resiliency Analysis Methodology (SCRAM). The MITRE Corporation, PR Case No. 16-0777, 2016, p.13.
9. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., Kott, A. Resilience metrics for cyber systems. Environment Systems and Decisions, 2013, No. 33(4), pp. 471-476.
10. Bodeau, D.J., Graubart, R. D. Cyber resiliency design principles: selective use throughout the lifecycle and in conjunction with related disciplines. The MITRE Corporation, Tech. Rep., 2017, p.98.
11. Drozd, O., Kharchenko, V., Rucinski, A., Kochanski, T., Garbos, R., Maevsky, D. Development of Models in Resilient Computing. In: 10th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2019, pp. 1-6.
12. Guelfi, Nicolas. A formal framework for dependability and resilience from a software engineering perspective. Central European Journal of Computer Science, 2011, No. 1, pp. 294-328.
13. Giudice, M., Wilkinson, C. Crowe Horwath. Resilience Going Beyond Security to a New Level of Readiness, 2016. Available at: https://www. crowehorwath.com/insights/asset/cyber-resilience-readiness-level (accessed 9.01.2020).
14. Linkov, I., Palma-Oliveira, J. M. (Eds.) Resilience and risk: Methods and application in environment, cyber and social domains. Springer, 2017. 580 p.
15. Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., Stavrou, A. A moving target DDoS defense mechanism. Computer Communications, vol. 46, 2014, pp. 10-21.
16. Javadianasl, Y., Manaf, A. A., Zamani, M. A Practical Procedure for Collecting More Volatile Information in Live Investigation of Botnet Attack. In: Multimedia Forensics and Security, Springer, 2017, pp. 381-414.
17. Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., Khayam, S. A. A taxonomy of botnet behavior, detection, and defense. IEEE communications surveys & tutorials, 2014, vol. 16, no. 2, pp. 898-924.

18. Bhuyan, M. H., Bhattacharyya, D. K., Kalita, J. K. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognition Letters, vol. 51, 2015, pp. 1-7.

19. Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., Kalita, J. K. Network attacks: Taxonomy, tools and systems. Journal of Network and Computer Applications, vol. 40, 2014, pp. 307-324.

20. Wang, B., Zheng, Y., Lou, W., Hou, Y. T. DDoS attack protection in the era of cloud computing and software-defined networking. Computer Networks, vol. 81, 2015, pp. 308-319.

21. Pathan, A. S. K. (Ed.). Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 2016. 638 p.

22. Branitskiy, A., Kotenko, I. Network Attack Detection Based on Combination of Neural, Immune and Neuro-Fuzzy Classifiers. In: 2015 IEEE 18th International Conference on Computational Science and Engineering (CSE), 2015, pp. 152-159.

23. IMPERVA INCAPSULA. Available at: https://www.incapsula.com/ddos/attack-glossary (ac-cessed 9.11.2019).

24. Najafabadi, M. M., Khoshgoftaar, T. M., Napolitano, A., Wheelus, C. RUDY Attack: Detection at the Network Level and Its Important Features. In: FLAIRS Conference, 2016, pp. 288-293.

25. Pedrycz, W., Waletzky, J. Fuzzy clustering with partial supervision. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 1997, vol. 27, no. 5, pp. 787-795.

26. VIRUS BULLETIN. Grooten, M. VB2017 videos on attacks against Ukraine, 2017. Available at: https://www.virusbulletin.com/blog/2017/12/vb2017-videos-attacks-against-ukraine/ (accessed 9.01.2020).

27. SOURCE FORGE. R-U-Dead-Yet? (RUDY) Original source code files. Available at: https:// sourceforge.net/projects/r-u-dead-yet/ (accessed 9.01.2020).

28. SOURCE FORGE. Hyenae. Available at: https://sourceforge.net/projects/hyenae/ (accessed 9.01.2020). dsniff. Available at: https://www.monkey.org/ ~dugsong/dsniff (accessed 9.11.2019).

Рецензія/Peer review : 04.12.2019 Надрукована/Printed : 02.01.2020