УДК 004.75 (004.5)

РОЗПОДІЛЕНІ СИСТЕМИ ВИЯВЛЕННЯ WORM-ВІРУСІВ

Богдан Савенко[1], Антоніна Каштальян[2],Наталя Петляк[3]
Хмельницький національний університет
[1]savenko_bohdan@ukr.net, [2]yantonina@ukr.net, [3]npetlyak@khmnu.edu.ua

В комп'ютерних мережах може перебувати різноманітне зловмисне програмне забезпечення. Завдяки технологіям та засобам підтримки функціонування комп'ютерних мереж, крім корисного їх застосування, наявні широкі можливості їх використання зловмисниками. Наприклад, для створення бот-мереж зловмисники можуть використовувати стандартні засоби роботи з пересилання повідомлень та файлів, команди, а також можуть для досягнення своєї мети, щоб приховати свої зловмисні дії, використати мережні віруси для проникнення у вузли в мережах та встановлення в них контролю. Такими вірусами можуть бути worm-віруси.

Метою даної роботи є покращення виявлення worm-вірусів завдяки використанню, крім методу виявлення, особливостей архітектури розподілених систем виявлення, в яку імплементовано метод виявлення.

Розподілена система виявлення зловмисного програмного забезпечення синтезована згідно принципів самоорганізації, адаптивності і часткової централізації. Розглянемо результати її застосування до worm-вірусів. Визначальною їх особливістю є спрямування на інфікування переважно комп'ютерів, а не файлів в них, і цільова функція спрямована саме на досягнення максимізації інфікування кількості комп'ютерів, а не файлів в них. Хоча можуть бути і такі, що додатково спрямовані на інфікування файлів в комп'ютерних станціях, в які отримали доступ. Маючи такий функціонал у worm-вірусах щодо їх поширення і спрямування саме для поширення в комп'ютерних мережах, як локальних так і глобальних, зловмисники можуть їх використати для цілеспрямованого охоплення корпоративної мережі, яка їх цікавить та, як наслідок, навколо якої можуть створити зони поширення таких worm-вірусів. Тому, захищаючи корпоративну мережу частково централізованими системами потрібно імплементувати в них підсистеми та засоби протидії такому зловмисному програмному забезпеченню, як worm-віруси. Введемо множину W_W комп'ютерних worm-вірусів так:

$$W = \{w_1, w_2, \dots, w_{N_w}\} W = \{w_1, w_2, \dots, w_{N_w}\}, \quad (1)$$

де $w_i w_i$ - ii - worm-вірус; $N_w N_w$ – кількість відомих worm-вірусів.

Задамо характеристичні показники worm-вірусів множиною $M_W = \{m_{W,1}, m_{W,2}, \dots, m_{W,N_W}\} M_W = \{m_{W,1}, m_{W,2}, \dots, m_{W,N_W}\}$, де $N_W N_W$ – кількість характеристичних показників, $m_{W,i} m_{W,i}$ - i_i-ий

характеристичний показник, $i = 1,2,\dots,N_W i = 1,2,\dots,N_W$. Деталізуємо кожен характеристичний показник з метою подальшого поєднання їх елементів для задання відповідно типу worm-вірусів.

При виборі за характеристичний показник елементу $m_{W,1} m_{W,1}$ можна поділити всю множину worm-вірусів на такі класи: клас, в якому не міститься жодного елементу з характеристичним показником $m_{W,1,j} m_{W,1,j}$ ($j = 1,2,\dots,5 j = 1,2,\dots,5$), тобто клас, в якому відсутні worm-віруси, і позначимо його $K_W^0 K_W^0$; клас $K_W^j K_W^j$ ($j = 1,2,\dots,5 j = 1,2,\dots,5$), який визначатиметься характеристичним показником $m_{W,1,j} m_{W,1,j}$ ($j = 1,2,\dots,5 j = 1,2,\dots,5$), і всього таких класів буде п’ять; клас $K_W^6 K_W^6$, в який будуть віднесені елементи, для характеристики яких буде більше одного характеристичного показника $m_{W,1,j} m_{W,1,j}$ ($j = 1,2,\dots,5 j = 1,2,\dots,5$). Побудова класу $K_W^6 K_W^6$ може бути здійснена системою $S S$ в процесі її функціонування при виявленні багатовекторних worm-вірусів. Для віднесення об’єкту до класу $K_W^6 K_W^6$ система $S S$ повинна встановити його мінімум в двох класах з класів $K_W^j K_W^j$ ($j = 1,2,\dots,5 j = 1,2,\dots,5$). Формування класу $K_W^0 K_W^0$ можливе за умови помилкового віднесення worm-вірусів до нього при застосуванні систем виявлення. При правильно здійсненій класифікації worm-вірусів клас $K_W^0 K_W^0$ буде порожнім, тобто $K_W^0 = \varnothing K_W^0 = \varnothing$. Наявність елементів в класі $K_W^0 K_W^0$ буде означати помилковість спрацювання відповідного детектора та системи в цілому. Таким чином, всю множину worm-вірусів поділено на шість класів:

$$W = \bigcup_{j=1}^{6} K_W^j W = \bigcup_{j=1}^{6} K_W^j. \quad (2)$$

З системою, в яку було імплементовано метод виявлення worm-вірусів було проведено експеримент з виділенням класів worm-вірусів та джерел їх поширення. Результати експериментів подано в табл. 1 за типами worm-вірусів та варіантами джерел поширення задано в табл. 1.

Для оцінювання достовірності виявлення worm-вірусів системою S та імплементованим в неї методом, як цілісного бінарного класифікатора, було визначено чутливість та специфічність моделі і обчислено їх значення. У результаті

отримано True Positives Rate - 73,52%, рівень помилкових позитивних результатів - 9,07%, чутливість - 73,52%, специфічність - 90,92%.

Таблиця 1

Результати експериментів

Результат виявлення	Класи worm-вірусів, $j = 1,2,\dots$	Серії експерименту / Екземпляри класу												Разом
		1			2			3			4			
		1	2	3	4	5	6	7	8	9	10	11	12	
FN	$K_w^{0,j}$	344	320	302	376	345	267	307	298	267	348	317	393	3884
TP	K_w^j	911	915	837	897	853	934	892	946	932	976	831	864	10788
FP	$K_w^{j,p}$	184	198	129	115	124	160	214	253	94	172	208	84	1935
TN	$K_w^{j,r}$	1561	1567	1732	1612	1678	1639	1587	1503	1707	1504	1644	1659	19393

Оскільки значення специфічності є високим, то система S виявляє негативні випадки краще, ніж позитивні, бо чутливість є меншою порівняно з специфічністю.

Таким чином, застосування розробленого рішення за результатами проведених експериментів підтверджує можливість ефективного його використання при розробці і експлуатації нового типу систем виявлення.

УДК 004.623

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДОСТУПУ ДО ХМАРНИХ ОБЧИСЛЕНЬ ЗА ДОПОМОГОЮ БЛОКЧЕЙН ТЕХНОЛОГІЇ

Роман Ситник[1], Вікторія Гнатушенко[2]

Український державний університет науки і технологій

[1]r.sytnyk@outlook.com, [2]vvitagnat@gmail.com

Децентралізований механізм контролю доступу до хмарних ресурсів на основі блокчейну та Distributed Ledger Technology забезпечує більшу безпеку хмарних обчислень та можливість прозорого журналювання та моніторингу хмарних систем.

Метою даної роботи є поліпшення механізмів забезпечення безпеки доступу до хмарних обчислень за допомогою технологій блокчейну.

Блокчейн – це розподілена база даних, в якій кожен запис має в собі хеш попереднього, що захищає дані від зміни, таким чином, що зміна одного запису зробить невірним хеш в усіх наступних записах. Технологічною основою блокчейну є Distributed Ledger Technology (DLT). Ця технологія є розподіленою базою даних, яка зберігає записи транзакцій у кількох вузлах мережі, а чи не в