УДК 004.732.056

РОЗРОБКА МЕТОДУ ОЦІНКИ СТАНУ КОМП'ЮТЕРА НА БАЗІ АНАЛІЗУ СИСТЕМНИХ ПОДІЙ

С.Ю. Гавриленко**, *І.В. Шевердін

Національний Технічний Університет «Харківський політехнічний інститут», Харків, вул. Кирпичева 21, gavrilenko08@gmail.com

У статті запропоновано метод оцінки стану комп'ютера на базі аналізу системних подій операційної системи Windows 10. Проведено аналіз системних подій в звичайному режимі та при зараженні системи вірусами типу PetyaA та WannaCry. Базуючись на статистиці параметрів подій операційної системи було виявлено закономірності, котрі описують стан операційної системи. Отримана статистика надала можливість побудувати набір асоціативних правил для виявлення комп'ютерних вірусів. Для накопичення системних подій та для їх подальшого аналізу, побудовано антивірусний додаток. Для швидкого пошуку кожного фактору вірусної активності у антивірусному додатку, використано хеш-таблиці. Розроблене програмне забезпечення дозволило виявити описані у даній статті фактори зараження та блокувати виконання вірусного процесу.
Ключові слова: антивірусний захист, антивірусна система, аналіз системних подій, багаторівневі карти, аналіз процесів операційної системи, асоціативний аналіз.

В статье предложен метод оценки состояния компьютера на базе анализа системных событий операционной системы Windows 10. Проведен анализ системных событий в обычном режиме и при заражении системы вирусами типа PetyaA и WannaCry. Основываясь на статистике параметров событий операционной системы было выявлено закономерности, которые описывают состояние операционной системы. Полученная статистика предоставила возможность построить набор ассоциативных правил для обнаружения компьютерных вирусов. Для накопления системных событий и для их дальнейшего анализа, построено антивирусное приложение. Для быстрого поиска каждого фактора вирусной активности в антивирусном приложении, использовано хеш-таблицы. Разработанное программное обеспечение позволило выявить описанные в данной статье факторы заражения и блокировать выполнение вирусного процесса
Ключевые слова: антивирусная защита, антивирусная система, анализ системных событий, многоуровневые карты, анализ процессов операционной системы, ассоциативный анализ.

In the article the method of an estimation of a computer condition on the basis of the analysis of system events of operating system Windows 10 is offered. The analysis of system events was performed in the normal mode and when the system was infected by viruses such as PetyaA and WannaCry. Based on the statistics of the parameters of the operating system events, regularities was found that describe the state of the operating system. The obtained statistics provided an opportunity to build a set of associative rules for detecting computer viruses. To accumulate system events and for their further analysis, anti-virus application are built. To quickly search for each factor of virus activity in an antivirus application, a hash table was used. The developed software allowed us to identify the infection factors described in this article and block the execution of the virus process
Key words: antivirus protection, antivirus system, system events analysis, multi-level maps, operating system processes analysis, associative analysis.

Вступ. Україна недоотримала 0,4% ВВП або 10 млрд гривень в зв'язку з кібератакою вірусу Petya, якому піддалися українські компанії 27 червня 2017 року. Вірус поширювався також в Росії, Англії, Індії та інших країнах Європи і Азії. Вже до 30 червня по всьому світу збитки від кібератаки склали 8 млрд доларів [1]. Аналіз елементарного монітору вірусної активності, показує, ці атаки відбуваються щосекунди. Обсяги комп'ютерних вірусів та шкідливого програмного забезпечення ростуть із загрозливою швидкістю. Нещодавно серед постраждалих від вірусу BadRabbit опинилися Київський метрополітен, де вийшла з ладу система банківських сервісів, і Одеський міжнародний аеропорт, де атаці піддалася інформаційна система, в зв'язку з чим виникли затримки рейсів. Крім того, хакери зачепили і Міністерство інфраструктури [2, 3].

Боротьба з вірусами стає одним із пріоритетних завдань. Незважаючи на усі зусилля дослідників і розробників у цій галузі, в даний час не існує такої антивірусної програми, яка могла б виявити всі вірусні загрози [4-10]. Саме тому питання розробки та вдосконалення антивірусних засобів залишається актуальною науковою задачею.

Метою статті є розробка системи виявлення комп'ютерних вірусів, яка базується на концептуальних принципах обробки системних подій операційної системи. Основна ідея роботи розробленого програмного забезпечення базується на поточному аналізі комп'ютерної системи та аналізі подій процесів виконання програмного забезпечення.

Результати розробки та досліджень. Для збору подій комп'ютерної системи використано програмний додаток "Process Monitor", для аналізу зібраної статистики –"Deductor Studio Academic". Розглянуто наступні поля подій операційної системи Windows 10: Time of Day, Process Name, PID, Operation, Path, Result, Detail, Date & Time, Relative Time, Duration, Completion Time, Event Class, Sequence, Image Path, Company, Description, Version, User, Authentication ID, Session, Command Line, TID, Virtualized, Integrity, Category, Parent PID, Architecture, проаналізовано події вірусних команд та зібрано статистику.

Для аналізу та відображення даних використано програмний додаток Deductor Studio Academic [11].

Проаналізовано наступні поля: Process Name, Result, Image Path, Event Class, Company, Version, Authentication ID, Category. Дані поля є найбільш інформативними та описують зміну системного стану.

Зібрано статистику роботи комп'ютерної системи в звичайному режимі та інфікованої вірусами PetyaA та WannaCry.

Аналіз різниці роботи інфікованої (рис. 2) та неінфікованої (рис. 1) комп'ютерної системи показав виконання системних процесів, які при штатній роботі не було виявлено. Як можливо побачити на (рис. 2) з'явився вірусний процес "PetyaA.exe", котрий активно використовує процес "rundll32.exe" системи Windows за допомогою якого він завантажує вірус "PetyaA.dat" та починає виконання системних операцій, такий як модифікація реєстру, зміна MBR та інше. Аналіз та відстеження за системним програмним додатком "rundll32.exe" та за його параметрами дозволяє попередити запуск шкідливого програмного додатку.

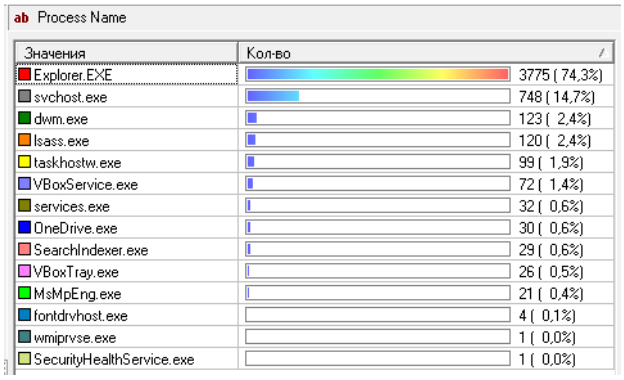


Рисунок 1 – Статистика процесів в неінфікованій операційній системі

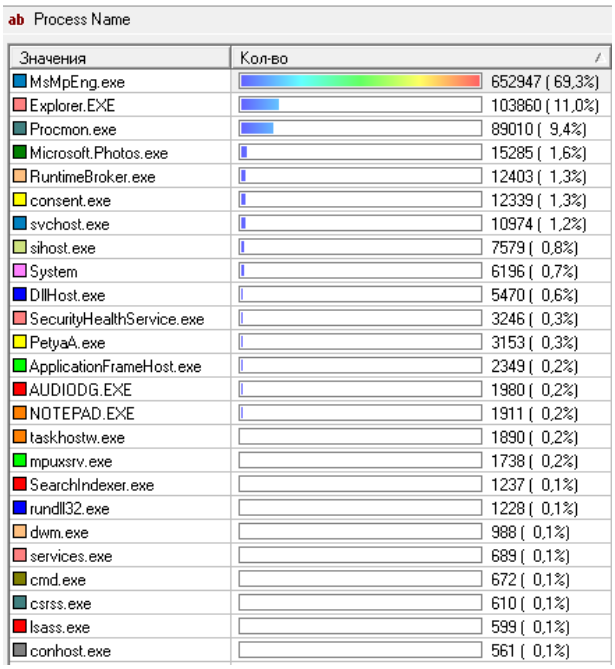
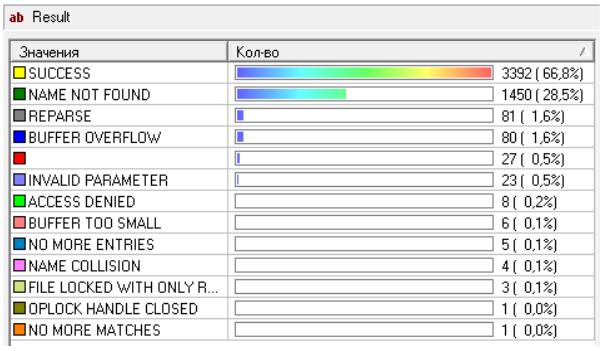


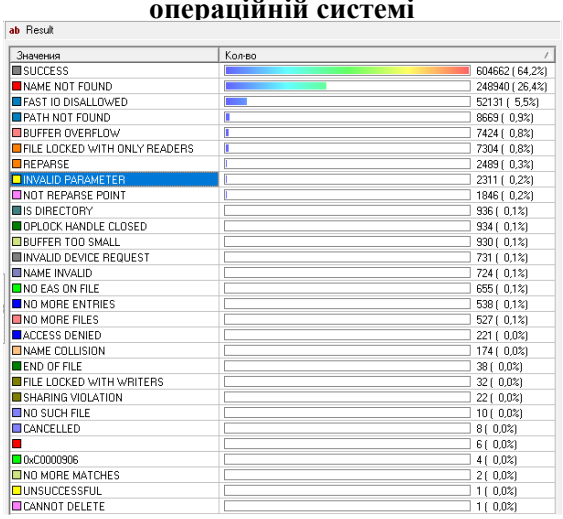
Рисунок 2 – Статистика процесів в інфікованій операційній системі

Іншим важливим індикатором зараження системи є аналіз результату виконання команд (рис. 3). У випадку інфікування системи вірусом змінюються результуючі значення системи (рис. 4), а саме INVALID PARAMETER, INVALID DEVICE REQUEST, NAME INVALID, NO EAS ON FILE, ACCESS DENIED, 0xC0000906, UNSUCCESSFUL, CANNOT DELETE, значення результату котрих є відмова у доступі, тільки запис, тощо.


ab Result

Значения	Кол-во
SUCCESS	3392 (66,8%)
NAME NOT FOUND	1450 (28,5%)
REPARSE	81 (1,6%)
BUFFER OVERFLOW	80 (1,6%)
	27 (0,5%)
INVALID PARAMETER	23 (0,5%)
ACCESS DENIED	8 (0,2%)
BUFFER TOO SMALL	6 (0,1%)
NO MORE ENTRIES	5 (0,1%)
NAME COLLISION	4 (0,1%)
FILE LOCKED WITH ONLY R...	3 (0,1%)
OPLOCK HANDLE CLOSED	1 (0,0%)
NO MORE MATCHES	1 (0,0%)

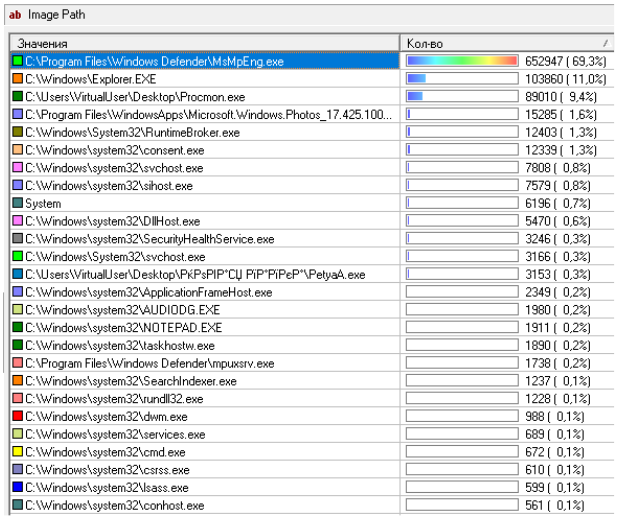
Рисунок 3 – Статистика результатів виконання команд в неінфікованій операційній системі


ab Result

Значения	Кол-во
SUCCESS	604662 (64,2%)
NAME NOT FOUND	248940 (26,4%)
FAST IO DISALLOWED	52131 (5,5%)
PATH NOT FOUND	8669 (0,9%)
BUFFER OVERFLOW	7424 (0,8%)
FILE LOCKED WITH ONLY READERS	7304 (0,8%)
REPARSE	2489 (0,3%)
INVALID PARAMETER	2311 (0,2%)
NOT REPARSE POINT	1846 (0,2%)
IS DIRECTORY	936 (0,1%)
OPLOCK HANDLE CLOSED	934 (0,1%)
BUFFER TOO SMALL	930 (0,1%)
INVALID DEVICE REQUEST	731 (0,1%)
NAME INVALID	724 (0,1%)
NO EAS ON FILE	655 (0,1%)
NO MORE ENTRIES	538 (0,1%)
NO MORE FILES	527 (0,1%)
ACCESS DENIED	221 (0,0%)
NAME COLLISION	174 (0,0%)
END OF FILE	38 (0,0%)
FILE LOCKED WITH WRITERS	32 (0,0%)
SHARING VIOLATION	22 (0,0%)
NO SUCH FILE	10 (0,0%)
CANCELLED	8 (0,0%)
	6 (0,0%)
0xC0000906	4 (0,0%)
NO MORE MATCHES	2 (0,0%)
UNSUCCESSFUL	1 (0,0%)
CANNOT DELETE	1 (0,0%)

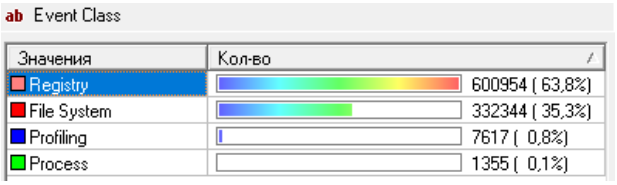
Рисунок 4 – Статистика результатів виконання команд в інфікованій операційній системі

Аналіз директорії розташування програми, котра виконується, надає статистику виконання системних процесів. Системні компоненти на програми знаходяться у системних директоріях таких як “C:\Windows\”, “C:\Windows\system32”, “C:\Windows\system32\drivers” та інші. Наявність в даних директоріях подій видалення, модифікації чи створення файлів є сигналом для перевірки процесів, які використовують ці події (рис. 5). Ще одною базовою характеристикою зараження є статистика виконання операцій роботи з системним реєстром, файловою системою, профайлінгом системи та роботи з процесами. Порівняльний аналіз подій між інфікованою (рис 6.) системою та неінфікованою (рис. 7) показав, що кількість операцій з системним реєстром збільшилася у 140 разів, робота з файловою системою зросла майже в 500 разів, кількість виконаних системних процесів зросла у 28 разів.


ab Image Path

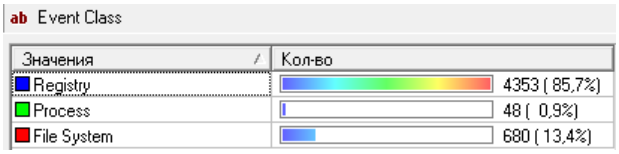
Значения	Кол-во
C:\Program Files\Windows Defender\MsMpEng.exe	652947 (69,3%)
C:\Windows\Explorer.EXE	103860 (11,0%)
C:\Users\VirtualUser\Desktop\Procmon.exe	89010 (9,4%)
C:\Program Files\WindowsApps\Microsoft.Windows.Photos_17.425.100...	15285 (1,6%)
C:\Windows\System32\RuntimeBroker.exe	12403 (1,3%)
C:\Windows\system32\consent.exe	12339 (1,3%)
C:\Windows\system32\svchost.exe	7808 (0,8%)
C:\Windows\system32\sihost.exe	7579 (0,8%)
System	6196 (0,7%)
C:\Windows\system32\DllHost.exe	5470 (0,6%)
C:\Windows\system32\SecurityHealthService.exe	3246 (0,3%)
C:\Windows\System32\svchost.exe	3166 (0,3%)
C:\Users\VirtualUser\Desktop\PkPsPIP°CЏ PiP°PiPeP°\PetyaA.exe	3153 (0,3%)
C:\Windows\system32\ApplicationFrameHost.exe	2349 (0,2%)
C:\Windows\system32\AUDIODG.EXE	1980 (0,2%)
C:\Windows\system32\NOTEPAD.EXE	1911 (0,2%)
C:\Windows\system32\taskhostw.exe	1890 (0,2%)
C:\Program Files\Windows Defender\mpuxsrv.exe	1738 (0,2%)
C:\Windows\system32\SearchIndexer.exe	1237 (0,1%)
C:\Windows\system32\rundll32.exe	1228 (0,1%)
C:\Windows\system32\dwm.exe	988 (0,1%)
C:\Windows\system32\services.exe	689 (0,1%)
C:\Windows\system32\cmd.exe	672 (0,1%)
C:\Windows\system32\csrss.exe	610 (0,1%)
C:\Windows\system32\lsass.exe	599 (0,1%)
C:\Windows\system32\conhost.exe	561 (0,1%)

Рисунок 5 – Статистика фізичного розтушування процесів на диску в інфікованій операційній системі


ab Event Class

Значения	Кол-во
Registry	600954 (63,8%)
File System	332344 (35,3%)
Profiling	7617 (0,8%)
Process	1355 (0,1%)

Рисунок 6 – Статистика операцій виконання команд з системним реєстром, файловою системою, профайлінгу системи та процесами в інфікованій операційній системі


ab Event Class

Значения	Кол-во
Registry	4353 (85,7%)
Process	48 (0,9%)
File System	680 (13,4%)

Рисунок 7 – Статистика операцій виконання команд з системним реєстром, файловою системою, профайлінгу системи та процесами в неінфікованій операційній системі

Останнім виділеним системним фактором є категорії. Категорії системно-операційних подій у інфікованій системі виділяється наступними факторами: ростом кількості неідентифікованих (прихованих) операцій, (рис. 8), з’являються операції запису метаданих та збільшується кількість операцій зчитування.

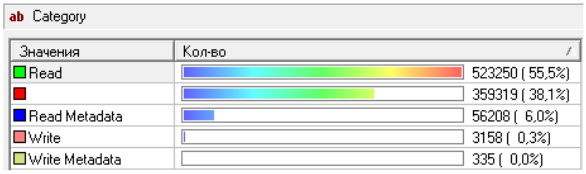


Рисунок 8 – Статистика категорії системно-операційних подій в інфікованій операційній системі

Після визначення стану виконується ідентифікація вірусного процесу. На даному етапі і виділяються процеси з сумнівними властивостями. Для цього виконується аналіз наступних параметрів подій: Company, Version, Authentication ID.

Аналізуючи підписи компаній, ми отримаємо інформацію о компанії, котра розробила даний програмний додаток. Як правило віруси не мають ніяких підписів, тому з легкістю ідентифікуються за даним фактором (рис. 9). Наступним критерієм відбору є версія. У програмних додатках є версія, котра як і компанія є важливим індикатором. У вірусів не має версій та підписів, тому що розробники вірусів ведуть розробку анонімно та на модифікованих програмних платформах.

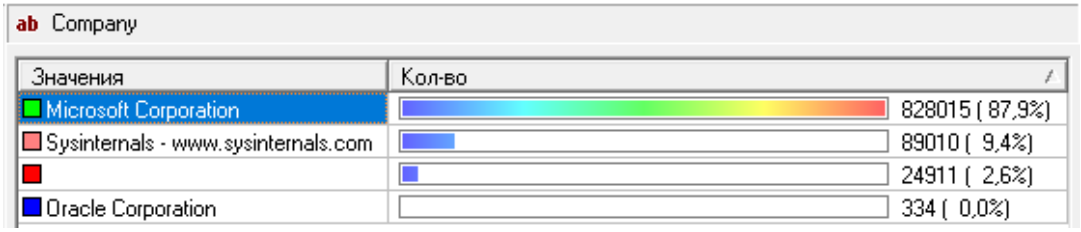


Рисунок 9 – Статистика підписів компаній в інфікованій операційній системі

Саме тому відсутність версії програмного додатку може бути ознакою шкідливого програмного забезпечення. На рис. 10 значення з відсутньою версією відображено червоним квадратом з кількістю операцій 24911.

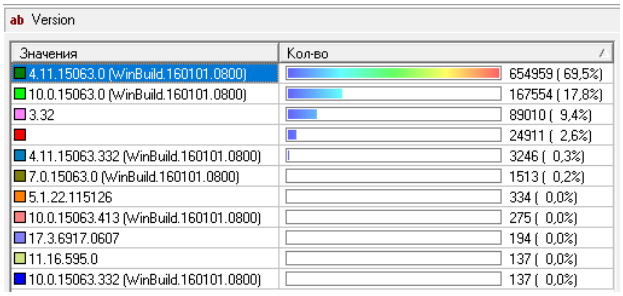


Рисунок 10 – Статистика версій програмних додатків в інфікованій операційній системі

Останній виділений фактор категорії є ідентифікатор запуску процесу. Аналізуючи статистику ідентифікатора запуску процесу, можливо ідентифікувати сервіс або користувача, котрий ініціював запуск процесу. У нашому випадку виділено ідентифікатор користувача “000e1346”, котрий до цього не мав такої кількості виконуючих процесів. При порівнявши інфікованої (рис. 11) та неінфікованої (рис. 12) системи видно що, ідентифікатор “000003e7” також збільшив кількість подій в 900 разів.

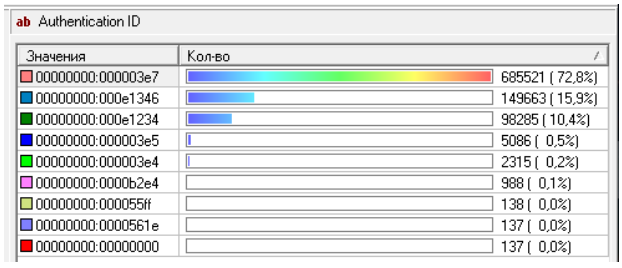


Рисунок 11 – Статистика ідентифікаторів запуску процесу в інфікованій операційній системі

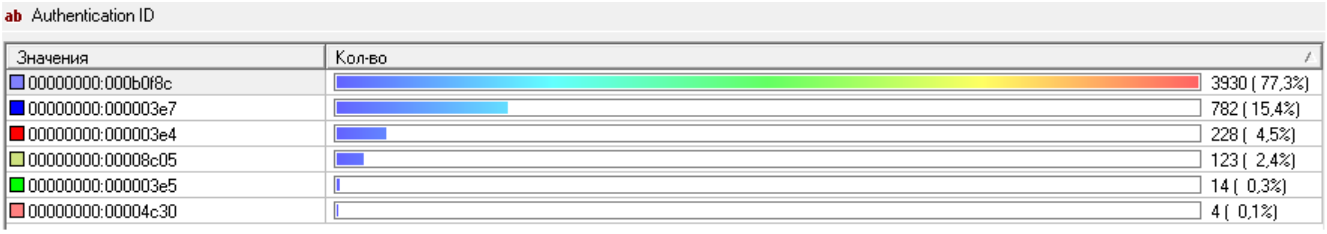


Рисунок 12 – Статистика ідентифікаторів запуску процесу в неінфікованій операційній системі

Отримані результати дозволили побудувати набір асоціативних правил системи виявлення комп'ютерних вірусів, базуючись на параметрах подій операційної системи, а саме Process Name, Result, Image Path, Event Class, Company, Version, Authentication ID, Category.

Параметрами, що описують стан системи є : Process Name, Result, Image Path, Event Class, Company. Параметри, що ідентифікують вірусний процес є: Version (версія програмного додатку), Authentication ID (ідентифікатор запуску процесу), Category (категорія системно-операційної події).

Нехай I = {i_i, i_2, ..., i_j, ..., i_n} – безліч (набір) параметрів (об'єктів) загальним числом n. Нехай D – безліч транзакцій D = {T_1, T_2, T_r, ..., T_m}, де кожна транзакція T – це набір елементів з I.

$$T = \{i_j \mid i_j \subset I\} \quad (1)$$

Ці параметри відповідають наступній множині об'єктів: I = { Process Name, Result, Image Path, Event Class, Company, Version, Authentication ID, Category }. Прикладами транзакцій можуть бути T_1 = { Process Name, Result, Image Path, Event Class, Company }, T_2 = { Version, Authentication ID, Category}. Множину транзакцій, в які входить об'єкт i_j, позначимо в такий спосіб:

$$D_{ij} = \{T_r \mid i_j \in T_r;\ j = 1\ldots n;\ r = 1\ldots m\} \subseteq D.$$

Деякий довільний набір об'єктів (ItemSet) позначимо в такий спосіб: $F = \{i_j \mid i_j \in I; j = 1..n\}$, наприклад F = { Company, Version }. Набір, що складається з k елементів, називається k-елементним набором. Множину транзакцій, в які входить набір F, позначимо в такий спосіб:

$$D_F = \{T_r \mid F \subset T_r;\ r = 1...m\} \subseteq D \quad (3)$$

Відношення кількості транзакцій, в яке входить набір F, до загальної кількості транзакцій (support) набору F позначимо як Supp(F):

$$Supp(F) = \frac{|D_F|}{|D|}. \quad (4)$$

Для множини { Company, Version } підтримка буде дорівнює 0,5, тому що даний набір входить в дві транзакції з номерами 1 і 2.

При аналізі виконано оцінку мінімального значення підтримки наборів $Supp_{min}$. Набір називається частим (large itemset), якщо значення його підтримки більше мінімального значення підтримки: Supp (F) > $Supp_{min}$. Таким чином, при пошуку асоціативних правил потрібно знайти множину всіх частих наборів:

$$L = \{F \mid Supp(F) > Supp_{min}\}. \quad (5)$$

Наприклад, для множини { Company, Version } = { "", 3.32 },

$$Supp(\{""\} \Rightarrow \{3.23\}) = \frac{2}{4} * 100\% = 50\%$$

Отже, підтримка правила рівна 50% (50% зі всіх транзакцій містять і «""», і «3.32»), а достовірність цього правила рівна 66.7% (66.7% зі всіх транзакцій, що містять «""», також містять і «3.32»).

Таким чином за результатами аналізу отримано наступні залежності: якщо в транзакції зустрівся деякий набір елементів F_1, то на підставі цього можна зробити висновок про те, що інший набір елементів F_2 також повинен з'явитися в цій транзакції. Алгоритми пошуку асоціативних правил призначені для знаходження всіх правил $F_1 \Rightarrow F_2$, причому підтримка і достовірність цих правил повинні бути вищою за деякі наперед задані пороги, тобто за мінімальну підтримку ($Supp_{min}$).

Результат виконання описаного алгоритму зображено на (рис. 12). Як видно із (рис. 12) розроблена програма реалізує запропонований алгоритм обробки та виводить системні події. При знаходженні асоціативного правила,

користувачу виводиться назва ідентифікованого вірусного процесу та інформаційне посилання про видалення інфікованого файлу процесу. У якості накопичувача системних подій використовується структура даних у вигляді черги. Побудова черги дозволяє виконати поетапний аналіз даних, а саме частина даних аналізується, друга частина накопичується для подальшого аналізу. Швидкий пошук елементів з вірусною сигнатурою виконується з використанням хеш-таблиці, наприклад, порівняння шляхів директорій та значень реєстру процесів. Для виділення частин строкових даних, таких як шлях до файлу виконання, ключі реєстру та детальний опис процесу, використано модель кінцевого автомату у вигляді RegExp.

Рисунок 13 – Результат виконання алгоритму у вигляді програмного додатку

Висновки.

Результатом роботи є розробка методу антивірусного захисту комп'ютера на базі аналізу системних подій операційної системи Windows 10. Проведено аналіз системних подій в звичайному режимі та при зараженні системи вірусами типу PetyaA та WannaCry. За допомогою кінцевого автомату виділено директорії виконання в полі події "Image Path. Поля подій містять дві частини, котрі описують стан системи та конкретну подію. Базуючись на статистиці параметрів подій операційної системи, виявлено закономірності, котрі описують стан операційної системи у звичайному режимі та при зараженні комп'ютерним вірусом. Отримана статистика надала можливість побудувати набір асоціативних правил для виявлення комп'ютерних вірусів. Для накопичення системних подій та для їх подальшого аналізу, побудовано антивірусний додаток. Для швидкого пошуку кожного фактору вірусної активності у антивірусному додатку, використано хеш-таблиці. Розроблено програмне забезпечення, яке дозволило проаналізувати сукупність подій, визначити стан системи, та при необхідності, прийняти рішення про видалення процесу.

1. Через атаки вірусу Petya Україна за півгодини втратила 10 млрд гривень [Электронный ресурс]. – Режим доступу до ресурсу: . https://www.segodnya.ua/economics/enews/iz-za-ataki-virusa-petya-ukraina-za-polchasa-poteryala-10-mlrd-griven-ekspert-1069181.html

2. Вирусная атака в Украине: в СБУ рассказали, как идет борьба с вирусом Сегодня 2017 [Электронный ресурс]. – Режим доступа к

ресурсу: https://www.segodnya.ua/ukraine/virusnaya-ataka-v-ukraine-v-sbu-rasskazali-kak-idet-borba-s-virusom-1066518.html

3. Киберполиция сообщила о последствиях вируса BadRabbit для Украины РИА Новости Украина 2017 [Электронный ресурс]. – Режим доступа к ресурсу: http://rian.com.ua/incidents/20171025/1028863477.html

4. Усовершенствованная концепция защиты данных на базе многоуровневого анализа карт операционной системы/ С.Ю. Гавриленко, И.В.Шевердин // Системи управління навігації та зв'язку. – Полтава, 2017, с. 8.

5. Семенов. С.Г. Защита данных в компьютеризированных управляющих системах (монография) / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко.– «LAP LAMBERT ACADEMIC PUBLISHING» Германия, 2014.– 236 с.

6. Лукацкий А.В. Обнаружение атак/А.В. Лукацкий. – Спб: BXB-Петербург, 2001. – 624 с.

7. Шелухин О.И. Обнаружение вторжений в компьютерные сети / О.И. Шелухин, Д. Ж Сакалема, А.С. Филинова. – М.: Гарячая линия-Телеком, 2013. – 220 с.

8. Gavrilenko S. Approximating computer system operation technologies under external action through the brusselator model with perturbation in the form of dynamic chaos / S. Semenov., S.Gavrilenko // Transilvania University of Brasov, Romania, Recent 44-Vol. 16 (2015), No. 1 (44), March 2015.– pp 36-40.

9. Gavrilenko S. Formation and study of heuristics in antivirus analyzers using the Mamdani algorithm / S.G. Semenov, S.YU. Gavrilenko // Journal of Qafqaz university, Azerbadhan, Mathematics and computer science 2015, Vol.(3), № 3, pp. 116-120.

10 Semenov S. Assessment of the state of the computer system based on the Hurst exponent/ S. Gavrilenko, S. Semenov, V. Chelak // Proceedings of the symposium "Metrology and metrology assurance"– Sozopol, Bulgaria, 2017, pp. 119-122.

11. Deductor Studio Academic [Электронный ресурс]. – Режим доступа к ресурсу: https://basegroup.ru/deductor/download.

Поступила в редакцію 11.05.2018 р.
Рекомендували до друку: докт.техн.наук, проф. Олійник А. П., докт. техн. наук, проф. Горбійчук М. І.