Conclusions. MySQL is more suitable for CRM systems where the database must be rigorously structured without the dynamic appearance of tables or schemas. A prerequisite is to use indexes in tables. MongoDB is more suitable for CRM systems where the database is dynamic in terms of data change, flexible, performs a large number of searches and has no rigid structure. In this case, the indexes do not play a big role.

REFERENCES:

1. N. Leavitt, "Will NoSQL databases live up to their promise?" [Text], Journal Computer, - IEEE Computer Society Press Los Alamitos, CA, USA, vol. 43, no. 2, pp. 12 –14, feb. 2010.
2. D. Bartholomew, "SQL vs. NoSQL," [Text], Linux Journal, - Department of Computer Science, Maharaja Surajmal Institute of Technology, Janakpuri, N.delhi 110058, Indiano. 195, July 2010.
3. S. Sakr, A. Liu, D. Batista, and M. Alomari, "A survey of large scale data management approaches in cloud environments," [Text] Communications Surveys Tutorials - IEEE, vol. 13, no. 3, pp. 311–336, 2011.
4. R. Hecht and S. Jablonski, "NoSQL evaluation: A use case oriented survey" [Text], in Cloud and Service Computing (CSC), - 2011 International Conference on, dec. 2011, pp. 336 –341.
5. A. Boicea, F. Radulescu, and L. I. Agapin, "MongoDB vs Oracle – database comparison" [Text], in Emerging Intelligent Data and Web Technologies (EIDWT), - 2012 Third International Conference on, sept. 2012, pp. 330 –335.
6. B. F. Cooper, A. Silberstein, E. Tam, R. Ramakrishnan, and R. Sears, "Benchmarking cloud serving systems with ycsb" [Text], in Proceedings of the 1st ACM symposium on Cloud computing, - ser. SoCC '10. ACM, 2010, pp. 143–154.

УДК 004.056.5: 004.414.22

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДІВ ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОГРАМНИХ ЗАСОБІВ

М.Д. Даценко, С.В. Машурка
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Щороку в світі створюється величезна кількість комп'ютерних програм. Разом з цим зростає кількість комп'ютерних вірусів. Згідно зі звітом McAfee Labs [1] за перший квартал 2019 року в світі з'явилося понад 65 млн одиниць шкідливого програмного забезпечення (далі ШПЗ). Дані приведені на Рис. 1. Це на 18% більше, ніж за останній квартал 2018 року. При цьому загальна кількість ШПЗ практично досягло 1 млрд. Однією з причин цього явища є можливість автоматизованої розробки шкідливих програм. Про це свідчить і дані Data Breach Investigation Report за 2016 рік [2]. У звіті сказано, що більше 99% шкідливих програм існують у незмінному вигляді протягом 58 секунд і менше. При цьому більшість програм виявляються лише одного разу.

Ці дані свідчить про те, наскільки швидко зловмисники змінюють ШПЗ. Основним вектором атаки на даний момент є ШПЗ. При цьому, більшість зловмисників використовують більше одного вектора атаки [3]. Згідно з підрахунками міжнародних експертів, кожні 14 секунд у світі відбувається одна кібератака. У 2016 році цей час був 40 секунд. А прогноз на 2021 рік - 11 секунд. Однією з причин такого зростання фахівці вважають технологічні тренди. Згідно зі звітом компанії Cisco за 2018 рік [4], злочинці під час веб-атак в період 2014-2017 років широко використовували виконавчі файли а також шкідливий веб-контент.

Таким чином, необхідним і актуальним завданням в боротьбі з ШПЗ є визначення сильних та слабких сторін методів виявлення ШПЗ, а також систем, для яких той чи інший метод буде давати кращі результати.

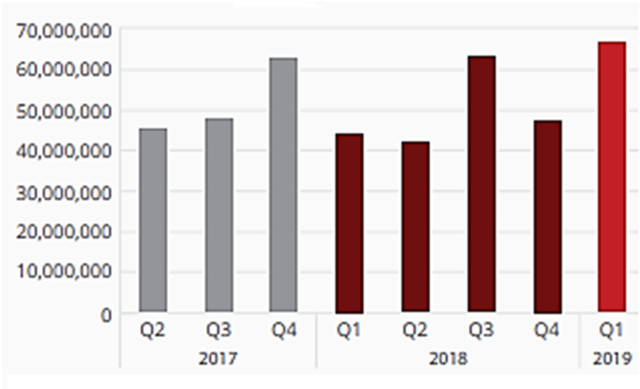

Рис.1. Графік росту кількості шкідливого програмного забезпечення

Основними методами виявлення ШПЗ є сканування, евристичний аналіз, виявлення змін та використання резидентних сторожів [5].

Сканування – це історично один із перших методів виявлення ШПЗ. При скануванні, програма-сканер проглядає вміст файлів на жорсткому диску, а також оперативну пам’ять пристрою. Класичне сканування передбачає пошук ШПЗ за їх сигнатурами. Сигнатура – це певна послідовність байтів, характерна для даного ШПЗ .

Основною перевагою даного способу є те, що він здатен виявляти широкий спектр ШПЗ а також висока швидкість роботи, яка зумовлена невеликою обчислювальною складністю.

До недоліків варто віднести те, що:

– сканування дозволяє виявити лише те ШПЗ, яке не використовує шифрування власного коду та поліморфізм;
– постійне використання ресурсів обчислювальної системи;
– необхідність постійного оновлення бази сигнатур;
– неможливо виявити ШПЗ, сигнатури якого немає в базі.

Евристичний аналіз. Суть цього методу полягає в контролі усіх дій, які може виконати програма, що перевіряється. При цьому відстежуються потенційно небезпечні дії, характерні для ШПЗ. Контролюючи дії програм, що перевіряються, аналізатор здатен виявляти нове ШПЗ ще до початку його виконання.

До недоліків даного методу слід віднести те, що

– евристичний аналізатор не дає повної гарантії виявлення будь-яких нових вірусів;

– постійне використання ресурсів обчислювальної системи;

– можлива помилкова тривога, коли аналізатор приймає безпечну програму за ШПЗ.

Метод виявлення змін. Базується на використанні програм ревізорів. Ці програми визначають і запам'ятовують характеристики всіх областей на дисках, в яких зазвичай розміщуються віруси. Під час періодичного виконання, програма-ревізор визначає нові характеристики контрольованих областей і порівнює їх з даними в пам’яті. У результаті порівняння, програма дає відповідь про можливу наявність ШПЗ.

Зазвичай програми-ревізори запам'ятовують наступні параметри:

– образи головного завантажувального запису;

– образи завантажувальних секторів логічних дисків;

– характеристики всіх контрольованих файлів і каталогів;

– номера дефектних кластерів;

– обсяг встановленої оперативної пам'яті;

– кількість підключених до комп'ютера дисків і їх параметри.

Перевагами методу є можливість виявлення ШПЗ усіх типів, в тому числі і так званих «стелс-вірусів», а також нове невідоме ШПЗ. Окрім цього використання даного способу може прискорити роботу інших методів виявлення ШПЗ. Наприклад, можна сканувати лише ті файли, які зазнали змін.

Метод виявлення змін має один суттєвий недолік: за допомогою програм-ревізорів неможливо визначити ШПЗ у файлах, які надходять в систему вже зараженими. ШПЗ буде виявлено лише після розмноження.

Метод використання резидентних сторожів. Заснований на застосуванні програм, які постійно перебувають в ОП ЕОМ і відстежують дії інших програм. Метод дозволяє виявити виконання підозрілих дій , таких як звернення для запису в завантажувальні сектора, розміщення в ОП резидентних модулів, спроби перехоплення переривань і т.п. До переваг методу можна віднести теоретичну можливість виявляти ШПЗ будь-якого типу, а також виявлення ШПЗ в момент виконання небезпечної дії.

Недоліком є практична неможливість реалізації повного контролю, а також значний відсоток помилкових тривог.

Висновки. Розглянувши основні методи виявлення шкідливого програмного забезпечення можна зробити висновки про те, що метод сканування гарно підходить для систем, які мають постійну можливість оновлення своїх баз вірусних сигнатур. Якщо дана вимога не виконується – втрачає сенс використання даного методу в будь-якій системі.

Метод евристичного аналіз ідеально підходить для систем, в яких циркулює велика кількість шифрованого трафіку та в системах, в яких немає жорстких вимог до кількості помилок другого роду.

Метод виявлення змін підходить для будь-яких систем в якості методу, який пришвидшує роботу інших методів. Не підходить для встановлення на вже запущену систему, адже вразливий до атаки першого дня.

Метод використання резидентних сторожів підходить для систем, які постійно стикаються з великою кількістю нових вірусів. Не підходить для систем з малою кількістю обчислювальних ресурсів.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Mcafee labs threats report.: веб-сайт. URL:https://www.mcafee.com/ enterprise/en-us /assets/reports /rp-quarterly-threats-aug-2019.pdf (дата звернення: 14.11.2019)

2. Data Breach Investigation Report.: веб-сайт. URL: https://regmedia.co.uk/ 2016/05/12/ dbir_2016.pdf (дата звернення: 10.11.2019)

3. Data Breach Investigation Report.: веб-сайт. URL: https://www.cisecurity.org/ blog/top-10-malware-september-2019/ (дата звернення: 12.11.2019)

4. Data Breach Investigation Report.: веб-сайт. URL: https://www.cisco.com/ c/dam/global/ ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf (дата звернення: 13.11.2019)

5. Ахметов І.Г. Молодой ученый. Международный научный журнал. 2016. № 125. С. 758.

UDC 004.048

DEVELOPMENT AND STUDY OF INTERACTION TRADING PLATFORM WITH CONSUMERS

D. Slipko, A.T. Khar
(Ukraine, Dnipro, NTU «Dnipro Polytechnic»)

Introduction. This article is about website development and analysis. Allow to show the full cycle of sales of goods from the very beginning.

The aim of this work is to develop a website and analyze the effectiveness of the trading platform.

Relevance and implementation methods. The rapid development of the Internet, the use of the latest technology and communications in business and everyday life has led to the emergence of new economic phenomena, such as electronic commerce. Currently, trading electronic platforms of various types and purposes are widespread [1,2].

E-commerce in Ukraine is one of the newest and most promising forms of innovation in the field of trade [3]. With the help of electronic commerce, most business processes are accelerated due to their electronic implementation, since information is transmitted directly to the recipient, bypassing the stage of creating a paper copy at each stage.