МЕТОДИ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ RANSOMWARE ЗАГРОЗ

Федюшин О. І., Хижняк К. М.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день на зміну фішинговим атакам через електронні листи чи то підроблені адреси сайтів приходять досить часто програми-вимагачі, які в своїй основі для розповсюдження шкідливого коду використовують схожі з фішинговими атаками технології. Але в багатьох випадках є більш шкідливими адже можуть спотворювати дані користувачів за допомогою шифрування, знищувати інформацію та надсилати повідомлення з погрозами [1]. Запобігти таким атакам складно, але можливо через проведення аналізу поведінки шкідливого програмного коду, а також проведення регулярного моніторингу мережної активності.

При виявленні програм-вимагачів і зловмисних програм виділяють методи на основі паттернів, які описують поведінку шкідливих програм на основі даних часу виконання коду шкідливої програми [2, 3]. Цю інформацію можна отримати попередньо з результатів динамічного аналізу програмного коду та додатково за результатами статичного аналізу.

Оскільки дані про час виконання крипто-вимагача зберігаються у файлах трасування у текстовій формі, ці файли можна переглядати як документи, і відповідно виклики API в цих файлах можна розглядати як терміни (слова).

Таким чином, для виявлення ознак програм-вимагачів в тому числі і крипто можна використовувати методи виявлення ознак подібні до аналізу текстів.

Метою доповіді є ознайомлення з методами виявлення та блокування ransomware-загроз на основі Bag of Words (BoW) методології виявлення ознак поведінки шкідливого коду. Для виявлення програм-вимагачів тут використовується техніка побудови n-gram для створення набору API функцій, які послідовно запускає програма-вимагач.

Результати досліджень показали, що ефективним способом для вирішення завдання є використання векторизації, яка дозволяє перетворити дані з текстового представлення у числову форму, і відповідно їх зафіксувати. В залежності від типу аналізу зафіксовані ознаки можуть бути або поведінковими, або структурними.

Список літератури

1. Сєвєрінов, О. В., Шевцов В. О., Сокол-Кутиловська А. С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка - 2017. - № 1. - С. 65-68.

2. Alqahtani, A.; Sheldon, F.T. A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. Sensors 2022, 22, 1837. DOI: https://doi.org/10.3390/s22051837.

3. Miao, Q.; Liu, J.; Cao, Y.; Song, J. Malware detection using bilayer behavior abstraction and improved one-class support vector machines. Int. J. Inf. Secur. 2016, 15, 361–379. DOI: https://doi.org/10.1007/s10207-015-0297-6.