Роман Щука
Аспірант,
Хмельницький національний університет, м. Хмельницький, Україна
ORCID: 0000-0003-4897-6320
schuka.roman@gmail.com

СУЧАСНІ МЕТОДИ ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОГРАМ

Анотація. У дослідженні здійснено аналіз поточного стану шкідливого програмного забезпечення (ШПЗ). Для цього вирішено три часткові задачі: класифіковано й описано основні типи ШПЗ, прийоми і методи боротьби з його окремими різновидами; розглянуто підходи до виявлення загроз; з'ясовано основні недоліки поширених методів викриття згубних програм. Отримані результати дозволили обґрунтувати необхідність пошуку нових шляхів боротьби з програмними небезпеками. В якості концептуальної основи для подальших досліджень запропоновано обрати методи штучного інтелекту. Вони,як на нашу думку, дозволили б виявляти ще не використовуване у хакерських атаках ШПЗ.

Ключові слова: шкідливе програмне забезпечення; ШПЗ; malware; N-грами; CFG-графи.

1. ВСТУП

Невпинний розвиток інформаційних технологій зумовлює перманентні зміни у способах комунікації із застосуванням мережевих технологій. Створення, зберігання, розповсюдження та спільне використання інформації стає дедалі більш простим, доступним і уразливішим. Останньою обставиною охоче користуються зловмисники.

Постановка проблеми. Розширення асортименту носіїв інформації, збільшення способів її поширення, розвиток операційних систем і системного ПЗ стимулює еволюцію ШПЗ і його урізноманітнення. Це призводить до збільшення вразливості інформаційних пристроїв за несанкціонованого доступу до них [1].

Аналіз останніх досліджень і публікацій.

Згідно з даними компанії McAfee Labs, яка вивчає кіберзагрози та займається дослідженням питань кібербезпеки, протягом останніх років темпи зростання чисельності нового ШПЗ прискорюються. У I кв. 2018 р. у середньому реєструвалось 5 нових шкідливих програм (ШП) за секунду; спостерігались суттєві технологічні зміни нових ШП; підвищувалася успішність прийомів зламу. Щодня сервіс McAfee Global Threat Intelligence аналізував 2,5 млн URL-адрес й понад 700 тис. файлів й оприлюднив наступну статистику [2]:

– за день в середньому виконувалось 51 млрд запитів;

– у I кв. 2018 р. захист від ШПЗ спрацьовував 79 млн разів на добу, порівняно з 45 млн у IV кв. 2017 р.;

– у I кв. 2018 р. захист від ризикованих URL-адрес спрацьовував 49 млн разів, що на 12 млн більше, ніж у попередньому кварталі;

– за той же час захист від ризикованих IP-адрес спрацьовував 36 млн разів проти 26 млн наприкінці 2017 р.

У II кв. 2018 McAfee GTI щодоби отримувало в середньому 49 млн запитів. Тоді ж спостерігався сплеск числа нового ШПЗ для мобільних пристроїв – кількість програм збільшилась на 27% порівняно з першим кварталом [3]. Динаміка появи нових ШП та зміни їх загальної кількості подано на рисунку 1.

У 2018 р. на тлі інших атак значно зросла кількість нових ШП, пов'язаних з добуванням криптовалют [4]. За останній квартал 2017 р. виявлення криптомайнингового ШПЗ збільшилось на 27%. За кількістю атак цей тип ШПЗ поступився лише рекламним ШП.

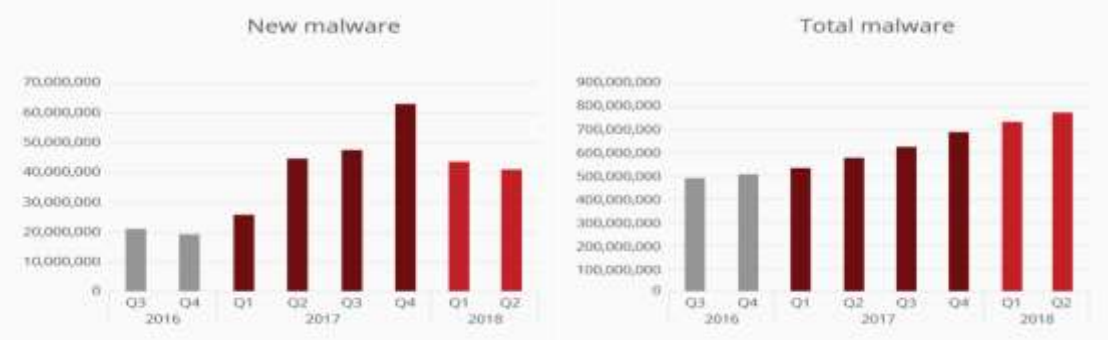

Рисунок 1. Кількість нових ШПЗ та загальна кількість ШПЗ [3]

Android'и виявились більш вразливими. Кількість нового криптомайнингового ШПЗ для них у I кв. 2018 р. порівняно з IV 2017 зросла у 40 разів (темп склав 4000%.)

Мета публікації. Враховуючи наведене, метою дослідження стала класифікація відомих програмних загроз та пошук найбільш ефективного інструментарію для боротьби із ними.

2. ТЕОРЕТИЧНІ ОСНОВИ

Зазвичай виявлення ШПЗ відбувається як "на стороні" мережі, так і "на стороні" хосту. У першому випадку присутність і дія програми-шкідника фіксується під час використання мережевого трафіку. У другому це відбувається на тлі застосування внутрішніх даних. Подібна обставина зумовлює появу двох типів аналізу ШП:

– статичного (код перевіряється без фактичного запуску програми на виконання);
– динамічного (додаток виконується у реальному чи у віртуальному середовищі).

Інша диференціація базується на виокремленні стратегій виявлення ШПЗ:

– за аномалією виконання (пошук відхилень від нормальної роботи програми);
– за неправомірним виконанням (виявляються неправомірні дії та поведінка).

Викладене вище дозволяє виділити три основні методи, що використовуються для виявлення ШПЗ — сигнатурні, поведінкові та евристичні.

3. МЕТОДИ ДОСЛІДЖЕННЯ

Сигнатурні методи (СМ). Описують кожну атаку власною моделлю (сигнатурою). В якості останньої застосовується:

– рядок символів;
– семантичні вирази на спеціальній мові;
– формальна математична модель тощо.

Сигнатури виділяють експерти (комп'ютерні вірусологи). Вони виокремлюють з програми код вірусу і у зручній для пошуку формі формулюють його характерні властивості. Майже кожна компанія, що розробляє антивіруси, має групу цих фахівців.

Алгоритм роботи методу заснований на пошуку сигнатур-атак у вихідних даних, зібраних мережевими і хостовими датчиками СВА (системи виявлення атак). Остання фіксує факт вірогідної атаки, що відповідає знайденому "підпису", та поновлює БДС (БД сигнатур). Усі вхідні файли перевіряються на наявність у них вірусного "підпису", що збігається з записом у БДС. Система захисту передбачає постійне оновлення БДС.

Цей метод є найбільш витребуваним при створенні комерційних антивірусів. Використовується у випадках, коли "підписи" відомі та задокументовані. Проте сигнатурні алгоритми не здатні розпізнати атаку нового ШПЗ [5]. Це викликає необхідність запровадження нових евристичних підходів.

Поведінкові методи (ПМ). Дозволяють приймати рішення щодо безпечності програм завдяки моніторингу їх роботи. Ґрунтуються на спостеріганні за діями додатків. Здатні нівелювати недоліки СМ, оскільки орієнтуються на те, що ШП робить, а не на те, що "говорить". Завдяки ПМ класифікують і програми однакової поведінки.

Поведінковий детектор утворюють такі компоненти [6]: Data Collector (збирає інформацію про виконуваний файл); Interpreter (перетворює її на представлення, придатні для подальшого аналізу); Matcher (порівнює представлення з підписами поведінки). Перевагою ПМ є можливість викриття ШПЗ, яке СМ детектувати не здатні.

Евристичні методи (ЕМ). ЕМ для виявлення ШПЗ застосовують підходи, подані на рисунку 2.

Рисунок 2 – Особливості використання евристичного методу

4. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Невідомі і метаморфічні сімейства ШП детектуються на основі оцінювання подібності графів (a simple graph similarity measurement). Зазвичай, виокремлюються опкоди з безпечних і вже уражених програм, створюється граф OpCodes, який дає можливість прогнозувати ймовірність шкідливості додатку.

Цікаві результати отримуються після поєднання фреймворку, що використовує метод загальних N-Gram (Common N-Gram), з класифікатором K-Nearest-Neighbour (KNN).

Підвищити ефективність виявлення ШПЗ, як на нашу думку, можна за використання графів контролю потоків (CFG). Комбінації API Calls, N-Gram, OPCode, Hybryd features і залучення можливостей штучного інтелекту видається нам перспективним напрямком подальших досліджень.

ПОСИЛАННЯ

[1] Abdullah A. Al-khatib, Waleed A. Hammood, "Mobile Malware and Defending Systems, Comparison Study", 2017.
[2] Christiaan Beek, Taylor Dunton, "McAfee Labs Threats Report", June 2018.
[3] Christiaan Beek, Carlos Castillo, "McAfee Labs Threats Report", Sept. 2018.
[4] Adam Kujawa, "Cybercrime tactics and techniques: Q1 2018", 2018.
[5] Saurabh Raje, Neil Wilson, Shyamal Vaderia, Rudrakh Panigrakhi, "Decentralised firewall for malware detection", 2016.
[6] Zahra Bazrafshan, Hashem Hashemi, Seyed Mehdi Hazrati Fard, Ali Hamzeh "A Survey on Heuristic Malware Detection Techniques", 2013