МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Інститут комп`ютерної інженерії, автоматизації, робототехніки та програмування ім.П.Н.Платонова

XXIV Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

18-19 квітня 2024 р.

Багато компаній використовують хмарні технології для роботи по обслуговуванню клієнтів, а також для зберігання й обробки важливих клієнтських даних. Успішна DoS-атака на хмарну інфраструктуру може спричинити відмову в обслуговуванні, серйозно вплинути на безліч бізнес-процесів та фактично паралізувати функціонування компанії. Таким чином, DoS-атаки, що вимагають оплати за їх припинення, стають значною загрозою для хмарних ресурсів компанії.

У подальшій перспективі, на думку аналітиків з McKinsey [4], ринок хмарних технологій у майбутньому буде тісно пов'язаний з інтернетом наступного покоління, відомим як Web 3.0, і зміниться під впливом технології блокчейн. Завдяки характеристикам блокчейна, таким як конфіденційність і децентралізація, очікується, що цей підхід посилить інформаційну безпеку та забезпечить надійну роботу ключових веб-ресурсів для бізнесу.

Висновок. Всупереч поширеному переконанню про безпеку та надійність хмарних сервісів, існує низка вразливостей, через які важливі дані можуть бути скомпрометовані. Відсутність контролю і прорахунки в системі безпеки можуть призвести до серйозних наслідків для бізнесу і приватних осіб. Тому необхідно враховувати та усувати такі вразливості, щоб забезпечити надійний захист своїх даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. AWS S3 Bucket Takeover Vulnerability: Risks, Consequences, and Detection URL: https://socradar.io/aws-s3-bucket-takeover-vulnerability-risks-consequences-and-detection/ (Доступ 22.03.2024)
2. What is zero trust architecture? how does it work? | Atera URL: https://www.atera.com/blog/what-is-zero-trust-architecture-how-does-it-work/ (Доступ 22.03.2024)
3. Google Cloud Threat Horizons Report Q3 2023.pdf URL: https://services.google.com/fh/files/blogs/gcat_threathorizons_full_oct2023.pdf (Доступ 23.03.2024)
4. What is Web3 technology (and why is it important)? | McKinsey URL: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-web3 (Доступ 24.03.2024)

УДК 004.49

МЕТОДИ ПОШИРЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

ФЕСЕНКО Т. М. (tanifesenko@gmail.com.), **ТОПЧІЙ Ю. П.** (ggeasywon@gmail.com)
Національний університет “Полтавська політехніка ім. Ю. Кондратюка”

У даній роботі здійснено аналіз сучасного стану шкідливого програмного забезпечення (ШПЗ). Для цього розв’язано три часткові задачі: класифіковано і описано основні типи ШПЗ, прийоми і методи боротьби з його окремими різновидами; розглянуто ряд сучасних підходів до виявлення кіберзагроз; з’ясовано основні недоліки поширених методів викриття деструктивного програмного забезпечення. Виконані дослідження дозволили обґрунтувати необхідність пошуку вразливостей інфокомунцікаційних активів та несанкціонованого доступу до них.

Постановка проблеми. Сьогодні будь-хто може стати жертвою атаки ШПЗ. У цьому контексті деякі користувачі знають, як розпізнати фішингові електронні листи та інше ШПЗ. Однак кібератаки є витонченими і постійно еволюціонують у міру вдосконалення технологій та безпеки. Шкідливі атаки також виглядають і функціонують по різному, залежно від типу ШПЗ. Наприклад, жертви атак руткітів можуть не знати про існування цього типу ШПЗ, оскільки воно розроблене таким чином, щоб залишатися невиявленим якомога довше.

За цих умов постає доволі суттєве питання щодо ідентифікації такого програмного забезпечення та методики убезпечення власних апаратно-програмних активів від несанкціонованого доступу, ураження даних або блокування пристрою.

Виклад суті дослідження. Згідно з даними компанії "McAfee Labs", яка вивчає кіберзагрози та займається дослідженням питань кібербезпеки, протягом останніх років зростання чисельності нового ШПЗ невплинно прискорюється.

Так, у першому кварталі 2022 року в середньому реєструвалось 5 нових шкідливих програм за секунду. Крім того, спостерігались суттєві технологічні зміни нового ШПЗ, внаслідок якого підвищувалась успішність прийомів зламу. Щодня сервіс McAfee Global Threat Intelligence аналізував 2 500 000 URL-адрес й понад 700 000 файлів. Така обставина обумовила наступну статистику:

- за день в середньому виконувалось 51 000 000 000 запитів;
- у першому кварталі 2022 року захист від ШПЗ спрацьовував 79 000 000 разів на добу, порівняно з 45 000 000 у четвертому кварталі 2021 року;
- у першому кварталі 2022 року захист від ризикованих URL-адрес спрацьовував 49 000 000 разів, що є на 12 000 000 більше, ніж за попередній квартал;
- у першому кварталі 2022 року захист від ризикованих IP-адрес спрацьовував 36 000 000 разів, в порівнянні з 26 000 000 за четвертий квартал 2021.

У другому кварталі 2022 McAfee GTI в середньому отримувало 49 000 000 000 запитів щодоби. У цей час також спостерігався сплеск чисельності нового ШПЗ для мобільних пристроїв – кількість програм збільшилась на 27% порівняно з першим кварталом.

За умов запуску ШПЗ можна завдати шкоди різними способами, зокрема:

- призвести до блокування пристрою та його непридатності для використання;
- крадіжки, видалення або шифрування даних;
- виконання пост експлуатаційних заходів захопленого пристрою;
- отримання облікових даних, які дозволяють отримати доступ до систем або служб якими ви користуєтесь;
- майнінг криптовалюти;
- використання платних послуг на основі отриманих даних (наприклад, телефонні дзвінки преміум-класу).

ШПЗ часто охоплює кілька категорій. Наприклад, програма може одночасно містити кейлогер, збирати паролі і бути хробаком для розсилки спаму.

Типи ШПЗ які найактивніше використовувались у зазначеному періоді:

- Фішингові атаки спрямовані на викрадення інформації щодо облікових даних під видом безпечного джерела електронної пошти, веб-сайтів, текстових повідомлень або інших форм електронного спілкування.
- Шпигунське програмне забезпечення. Інсталюючись без згоди користувачів може відстежувати їх активність в Інтернеті, збирати конфіденційну інформацію, змінювати параметри пристрою та зменшувати його продуктивність.
- Рекламне програмне забезпечення, застосовується для показу агресивної реклами, зазвичай у формі спливаючих оголошень.
- Віруси. Порушують сталу роботу пристроїв, перезаписуючи, пошкоджуючи або видаляючи дані на них.
- Руткіти використовувались для перехоплення контролю над стандартними процесами операційної системи та змінювали інформацію на вражених пристроях.
- Троянське програмне забезпечення. Принцип його дії установлення контролю над ураженим пристроєм/завантаження й інсталяція додаткового ШПЗ, на зразок вірусів або хробаків/використання ураженого пристрою для шахрайства/інше.
- Криптомайнінг, використовуються обчислювальні ресурси пристроїв для видобування криптовалют.
- Зловмисні програми з вимогою викупу спрямовані на знищення або блокування доступу до важливих даних.

Отже, виявлення ШПЗ може відбуватися 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 шкідливих програм:

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

І ще одна диференціація базується на виокремленні стратегій виявлення ШПЗ:

- аномалії виконання (полягає у пошуку відхилень від нормальної роботи програми);
- неправомірне виконання (зосереджується на конкретних неправомірних діях й поведінці).

Усе викладене вище дозволяє виділити три основні методи, що використовуються для виявлення ШПЗ. Це сигнатурні, поведінкові та евристичні методи. Для підвищення ефективності виявлення ШПЗ можна використовувати інші методи. Найбільшу цікавість, являють собою графи контролю потоків (CFG) та можливі комбінації розглянутих тут підходів. Всупереч тому, що вони залишилися поза межами нашого аналізу, вважатимемо їх дослідження напрямком для подальшої роботи. У цьому сенсі перспективним вважаємо і застосування можливостей штучного інтелекту.

Висновки. Таким чином, у даній роботі нами розглянуто динаміку розвитку ШПЗ, а також здійснено огляд ряду методів виявлення програм, які можуть становити загрозу для комп'ютерних систем. Визначено шляхи подальших досліджень у напрямі синергії досліджених методів з графами контролю потоків (CFG) та використання методів штучного інтелекту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Звіт з кібербезпеки 2023. Остерігайтеся звіту про штучного самозванця. URL: https://www.mcafee.com/en-us/resources/cybersecurity-reports-and-guides.html?csrc=vanity.
2. Шкідливі програми. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/vredonosnyye-programmy/.
3. Koval M., Sova O., Orlov O., Zhyvylo Y., Zhyvylo I. Improvement of complex resource management of special-purpose communication systems // 5(9-119) (2022): Eastern-European Journal of Enterprise Technologies. P. 34–44.

UDK 004.9

SOME PROBLEMS IN MANAGING SERVER COMPUTING RESOURCES USING DEEP MACHINE LEARNING TOOLS

O.KHOSHABA (Oleksandr.Khoshaba@gmail.com)
Vinnitsia National Technical University

Annotation. The paper examines some problems managing server computing resources using deep machine learning tools and shows the relevance of studying the problems and possible solutions. Particular attention is paid to the consideration of deep machine learning tools.

Formulation of the problem. The main goal of this work is to consider some problems of managing server computing resources using deep machine learning tools, to determine the relevance of studying them, and to suggest possible ways to solve them. Special attention should be paid to the consideration of deep machine learning tools.

Introduction. Managing server computing resources has become increasingly important due to growing data volumes, computational complexity, and the need for automation in infrastructure