УДК 004.056.53

Туржанська І. Д.

СУЧАСНИЙ СТАН ПРОБЛЕМИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІД ДАМПІНГУ

Вінницький національний технічний університет

Анотація

У статті розкрито поняття дампу пам'яті та процес дампінгу облікових записів. Також було досліджено сучасний стан проблеми захисту програмного забезпечення від дампінгу та було розглянуто можливі способи вирішення проблеми.

Ключові слова: дампінг, кібербезпека, інформаційні технології.

Abstract

The article explains the concept of memory dumping and the process of account dumping. The author also examines the current state of the problem of software protection against dumping and considers possible ways to solve the problem.

Keywords: dumping, cybersecurity, information technology.

Вступ

Захист програмного забезпечення від дампінгу став одним із найважливіших питань у сучасному цифровому світі. Оскільки технології продовжують стрімко розвиватися, зловмисники постійно шукають способи отримати неавторизований доступ до виконуваного коду програми, що загрожує безпеці, інтелектуальній власності та конфіденційності розробників. Оскільки зловмисники все ж знаходять нові методи та техніки, щоб обійти захист програмного забезпечення, ця проблема є актуальною в цей час. Тому було вирішено проаналізувати та висвітлити сучасний стан проблеми захисту програмного забезпечення від дампінгу.

Результати досліджень

Перед тим, як аналізувати проблему дампінгу потрібно ознайомитись з його визначенням. Отже, дамп пам'яті – це процес отримання всієї інформації, що міститься в оперативній пам'яті в певний момент, і запис її на накопичувач у вигляді файлу [1]. Дамп пам'яті зазвичай використовують для діагностики проблем всіх систем, щоб потім на основі зібраних даних усунути проблему раптової поломки системи.

З точки зору кібербезпеки, дамп пам'яті несе критичну цінність, адже він містить останню інформацію про роботу системи перед збоєм. І завдяки цим даним можна запустити ту частину програми, яка призначена для збору інформації про причини збою [2]. Розкриття цих даних дозволяє зловмисникам розробляти способи обходу захисту та незаконного використання програмного забезпечення. Це може призвести до піратства програмного забезпечення, порушення авторських прав, втрати інтелектуальної власності та фінансових втрат для розробників.

Програмний дампінг має свої особливості. Він включає в себе процес аналізу та злому виконуваного коду програми для отримання інформації про її функціональність, внутрішню логіку та алгоритми. Зловмисник може використовувати методи зворотного проектування, щоб отримати вихідний код або близьку копію. Злодії аналізують код, щоб знайти слабкі місця, які можуть бути використані для зламу систем безпеки або отримання несанкціонованого доступу.

Систему заходів, призначених для отримання інформації про облікові записи користувачів називають «дампінгом облікових даних», або «дампінгом паролів». Під час цього процесу зловмисник викрадає та копіює дані до заздалегідь визначеного сховища (як правило, на сервер). Після цього вважається, що облікові дані були "скинуті" [3].

Зазвичай кібератаки на дані облікових даних відбуваються в три етапи:

1) Зловмисник знаходить спосіб доступу до цільового пристрою.

2) Отримавши доступ, зловмисник шукає на пристрої збережені облікові дані. Зазвичай зловмисники розгортають шкідливе програмне забезпечення для збору комбінацій імені користувача та пароля.

3) Викрадені облікові дані зберігаються на заздалегідь визначеному сховищі для подальшого використання.

Поточна ситуація з антидампінговим захистом програмного забезпечення є складною, і заходи безпеки потребують постійного вдосконалення. Розробники програмного забезпечення та спеціалісти з кібербезпеки використовують широкий ряд комплексних заходів спрямованих на захист від дампінгових атак. Одним із способів вирішення цієї проблеми є використання методів обфускації та шифрування виконуваного програмного коду, або ж «механізми навісного захисту». Обфускація передбачає перетворення вихідного коду таким чином, що його важче проаналізувати та зрозуміти. Шифрування виконуваного коду захищає його від прямого доступу та аналізу, шифруючи та розшифровуючи його лише під час виконання програми. Такий спосіб максимально сповільнює, або ж іноді унеможливлює процес зчитування даних з дампу пам’яті. Навісний захист користується широкою популярністю зокрема через надійність та дешевизну підтримки.

Також пошерено використовують наступні механізми захисту [3]:

- Система виявлення вторгнень, яка виявляє підозрілу поведінку на сервері.
- CAPTCHA, за допомогою якої зменшується кількість користувачів-ботів, які використовуються для DDoS-атак.
- Багатофакторна аутентифікація, яка в разі отримання зловмисником доступу до даних облікового запису може не допустити вхід далі через відсутність одноразового пароля, який зазвичай приходить на раніше вказаний номер телефону користувача.
- Моніторинг журналів авторизацій та виявлення незвичних запитів на сервері.
- Використання систем на основі штучного інтелекту.

Окрім вищенаведених способів, спеціалісти з кібербезпеки використовують ще один підхід, який полягає у використанні антидампінгових заходів, призначених для ускладнення аналізу та видалення виконуваного коду з пам’яті під час роботи програми. Ці заходи можуть включати додаткові механізми для перевірки цілісності коду, перевірку наявності відкладника, застосування захисних оболонок навколо критичних розділів програми та інші методи.

Широке розповсюдження алгоритмів штучного інтелекту (ШІ) у сфері кібербезпеки, як і в цілому, свідчить про те, що з розвитком технологій можна суттєво вдосконалити існуючі реалізації або ж створити нові системи на основі ШІ, які самостійно, в режимі реального часу, поповнюватимуть та раціоналізуватимуть свій репозиторій виявленими ними вразливостями, щоб оперативно ліквідовувати наслідки кібератак. На мою думку, впровадження та заохочення технологій штучного інтелекту дозволить нам більш оперативно реагувати, усувати та запобігати різним загрозам кібербезпеки, пов'язаним не лише з дампінгом, а й з усіма питаннями загалом.

Висновок

В процесі дослідження можна відзначити, що наразі проблема дампінгу є досить актуальною, адже досі не знайдено жодного механізму, який би повністю усував цю проблему. Проте варто зазначити й те, що фахівці активно намагаються якомога краще посилити антидампінговий захист. Для цього було введено ряд комплексних заходів, зокрема: обфускація, шифрування вихідного коду, CAPTCHA, система навісного захисту, моніторинг вторгнень, аналіз та видалення коду з пам’яті тощо.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kirvan P. What is a memory dump? – TechTarget Definition [Електронний ресурс] / Paul Kirvan // WhatIs.com. – Режим доступу: https://www.techtarget.com/whatis/definition/memory-dump
2. В. А. Каплун О. В. Дмитришин Ю. В. Баришев. ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ (Частина 2) : навч. посіб. / В. А. Каплун О. В. Дмитришин Ю. В. Баришев. – Вінниця : ВНТУ, 2014.
3. Techslang. What is Credential Dumping? [Електронний ресурс]. Режим доступу: https://www.techslang.com/definition/what-is-credential-dumping/
4. Greenberg A. What Is Credential Dumping? [Електронний ресурс] / Andy Greenberg // WIRED. – Режим доступу: https://www.wired.com/story/hacker-lexicon-credential-dumping/
5. Artificial Intelligence in Cybersecurity – Examples | Codete Blog [Електронний ресурс] // Codete Blog. – Режим доступу: https://codete.com/blog/artificial-intelligence-in-cybersecurity-examples-of-use

Туржанська Ірина Дмитрівна – студентка групи 2БС-22Б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: turzhanskayaryna@gmail.com

Науковий керівник – Каплун Валентина Аполінаріївна

Turzhanska Iryna Dmitrievna – student of group 2BS-22B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: turzhanskayaryna@gmail.com

Supervisor – Kalpun Valentyna