УДК 004.056

О. Р. Паламарчук

МЕТОД ЗАХИСТУ ПРОГРАМ ВІД ДАМПІНГУ

Вінницький національний технічний університет;

Анотація

Розглянуто та проаналізовано поширені методи захисту програмних застосунків від дампінгу. Запропоновано власний метод для підвищення рівня модульності та можливості створення зашифрованих контейнерів, що дозволяє використовувати метод при розробці інших застосунків. Виявлено переваги та недоліки запропонованого методу.

Ключові слова: кібербезпека, дампінг пам'яті, шифрування.

Abstract

Common methods of protecting applications from memory dumping are considered and analyzed. An own method has been proposed to increase the level of software protection from such attacks. The advantages and disadvantages of the proposed method are revealed.

Keywords: cybersecurity, memory dumping, encryption.

Вступ

Сьогодні значною проблемою у сфері кібербезпеки є порушення конфіденційності користувачів, де зловмисники тим чи іншим чином використовують техніки дампінгу. Особливо важливим даний захист є в сфері захисту критичних даних, оскільки дампінг пам'яті може бути використаний для визначення вразливостей в програмному забезпеченні та пошуку точки входу для реалізації атаки, тому захист від несанкціонованого створення дампу пам'яті є одним з найважливіших методів захисту від несанкціонованого дослідження програмного забезпечення.

Метою роботи є покращення існуючих методів захисту програм від дампінгу.

Для досягення мети необхідно розв'язати такі задачі:

- проаналізувати існуючі методи для захисту програм від дампінгу;
- проаналізувати відомі засоби захисту програм від дампінгу;
- розробити власний метод комплексного захисту.

Результати дослідження

Більшість дамперів написаних для Windows використовують певний набір стандартних функцій призначених для роботи з процесами, такі як: OpenProcess(), ReadProcessMemory(), VirtualQueryEx(), які описані в заголовкових файлах processthreadsapi.h та memoryapi.h [1]. Для захисту програми від створення дампу логічно здійснити перехоплення даних функцій при зверненні до процесу програми. Іншим способом захисту від дампінгу є динамічне розпакування під час якого процес ніколи не перебуває в оперативній пам'яті повністю, оскільки антидампінговий модуль залишає розшифрованими тільки ті частинки програми, які зараз безпосередньо працюють, а ті які вже відпрацювали видаляються з пам'яті [1].

Запропоновано метод покращення захисту програмних застосунків від дампінгу за допомогою створення зовнішньої бібліотеки, яка буде містити в собі функції для захищеного зберігання даних в оперативній пам'яті та очищати ділянку пам'яті після закінчення роботи з нею. Робота бібліотеки починається не одразу після запуску програми, що її використовує, а лише після того як користувач створить об'єкт шифроконтейнеру та заповнить всі поля даного об'єкту. Далі метод захисту використовує поля об'єкту для визначення місця в оперативній пам'яті, куди потрібно здійснити запис та обчислення розміру даних, які потрібно туди записати. Наступним кроком методу захисту є встановлення перехоплення функцій, які намагаються отримати доступ до оперативної пам'яті процесу [2]. В цих процесах об'єктом виступає оперативна пам'ять, куди відбувається запис та

здійснюється перехоплення при спробі отримати доступ до ділянки, що виділена для процесу. Останнім кроком встановлення захисту є шифрування даних, які потрібно захистити.

Алгоритм роботи методу:

1) встановлення хуків для функції дампінгу;

2) генерування одноразового сесійного ключа для шифрування;

3) зашифрування захищуваних даних використовуючи даний ключ;

4) очищення ділянки оперативної пам'яті, де була записані дані до цього;

5) очікування використання даних та їх розшифрування;

6) закінчення роботи з даними та очищення оперативної пам'яті, де вони знаходились, а також зняття хуків з функцій дампінгу.

Даний метод має такі переваги над відомими:

- можливість мінімально змінювати вихідний код програмного застосунку для захисту;

Серед недоліків можна виділити:

- значне збільшення часу виконання програми при захисті даних великого обсягу;
- складно приховувати ключ шифрування в оперативній пам'яті;
- використання слабкого шифру [3].

В підсумку можна сказати, що даний метод попри недоліки варто використовувати на підприємствах, які розробляють програмні продукти, які потребують захисту від дампінгу. У той же час використання хуків може ускладнити розробку програмних продуктів, які використовують роботу з оперативною пам'яттю.

Висновки

Встановлено, що запропонований підхід дозволяє підвищити загальний рівень захищеності програми від дампінгу порівняно з стандартними методами захисту. Даний захист від дампінгу буде доцільно використовувати тим підприємствам, що розробляють додатки, які працюють з конфіденційними даними користувачів та розкриття яких може завдати підприємству значних репутаційних та фінансових втрат. Водночас даний захист не рекомендовано використовувати при розробці засобів, що часто використовують у своїй роботі читання та запис в оперативну пам'ять.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Каплун В.А., Дудатьєв А.В., Семеренко В.П. Захист програмного забезпечення. Частина 1 : навч. посіб. Вінниця : ВНТУ, 2005. 139 с.

2. MinHook - The Minimalistic x86/x64 API Hooking Library : URL : https://www.codeproject.com/Articles/44326/MinHook-The-Minimalistic-x-x-API-Hooking-Libra.

3. Тарнавський Ю.А. Технології захисту інформації : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.

Паламарчук Олександр Русланович — студент групи 2БС-22м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Науковий керівник: ***Баришев Юрій Володимирович*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Palamarchuk Oleksandr R. — student of 2БС-22м group, Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia,

Supervisor: ***Baryshev Yurii V.*** — PhD (Eng.), Associated professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia