УДК 004.056.53

ЗАХИСТ ВІД ДАМПІНГУ ШЛЯХОМ МОДИФІКАЦІЇ EXE-ЗАГОЛОВКА В ПАМ'ЯТІ

В. В. Шкурін, В. А. Каплун, ст. викладач
Вінницький національний технічний університет
scorpion333112@rambler.ru

У доповіді висвітлюється один з підходів до захисту від дампінгу програм і процесів. Актуальність здійсненої розробки модуля захисту від зняття програм з пам'яті підтверджується тим, що витрати виробників на створення більш ефективного методу захисту їх програмних продуктів компенсують потенційний збиток, що наноситься нелегальним копіюванням і використанням програм. При розробці комерційного програмного забезпечення багато фірм надають перевагу навісному методу захисту, ідея якого полягає в ускладненні аналізу роботи програми за допомогою шифрування коду програми і розшифровування його безпосередньо перед виконанням у пам'яті. При використанні такого захисту оригінальній код програми шифрується, модифікується PE-заголовок, до програми додається розшифровувач. Так працює переважна більшість програм-пакувальників. Перед виконанням програма розшифровується, частково відновлюється оригінальний PE-заголовок, керування передається програмі. Проте він легко зламується за допомогою знаходження моменту передачі керування оригінальній програмі та зняття дампу з її незашифрованого коду.

Таким чином, подібні методи захисту нічого не варті у тому випадку, коли зламник має можливість дослідити вміст основної оперативної пам'яті під час виконання програми і зняти зліпок пам'яті с метою

отримання "чистого" (без елементів захисту) шістнадцяткового коду програми. Отже, не може бути стійким захист програмного забезпечення, якщо не передбачити засоби протидії роботі дамперів.

Авторами доповіді для захисту від дампінгу пропонується використовувати методику зачистки PE-заголовку в образі виконуваного файлу в пам'яті. Якщо цей заголовок модифікувати певним чином або занулити, то образ програми, що зніметься з пам'яті за допомогою відомих програм-дамперів, буде недієздатний, оскільки важлива інформація для відновлення буде стерта, а отриманий виконуваний модуль буде непрацездатним, оскільки, як відомо, за завантаження програми у пам'ять відповідає саме заголовок.

Запропонований спосіб захисту виконаний у вигляді автономної програми і може бути без зайвих зусиль використаний при необхідності передбачити перешкоджання зняттю певної програми з пам'яті. Основними складовими цієї програми є такі: звернення до диспетчера задач, отримання списку процесів, зміна типу доступу до файлу, використання засобів для занулення PE-заголовку.

Звичайно, такий захист можна обійти і вручну відновити заголовок, але це вимагатиме певних знань та навичок зламника і певного часу. Крім того, авторами доповіді передбачається використання і інших антидампінгових методів, а саме: антидамп в нульовому кільці, динамічне розпакування та деякі інші.

Кожен спосіб захисту має ряд недоліків, якими може скористатися зловмисник для отримання даних з комп'ютера. Не дивлячись на свою простоту, запропонований захист може бути досить дієвим і, безумовно, ускладнить зловмиснику можливість зберегти дамп виконуваного процесу вигляді повноцінного шістнадцятого коду виконуваного модуля програми.