УДК 004.056.53

ОДИН З ПІДХОДІВ ДО ВИЯВЛЕННЯ КЛАВІАТУРНИХ ШПИГУНІВ І ЗАХИСТУ ВІД НИХ

В. В. Вітюк, В. А. Каплун, ст. викладач
Вінницький національний технічний університет
vova.vityk@gmail.com

З розвитком сучасних комп'ютерних технологій розвиваються не лише методики захисту інформації, але й способи її викрадення. Одним із способів несанкціонованого дослідження є так зване «шпигування», зокрема "клавіатурні шпигуни" (кейлогери), які утворюють велике сімейство шкідливих програмних та апаратних засобів, мета яких – шпигунство за роботою користувачів, зняття конфіденційної інформації. Сучасні кейлогери для своєї роботи використовують бібліотеки або драйвери, опитують клавіатуру, перехоплюють процеси, мають можливість передавання виявленої інформації по мережі Інтернет та використовують так звані руткіт-методи для забезпечення своєї непомітності в системі. Основні принципи роботи клавіатурних шпигунів такі: встановлення хуку перехоплення повідомлень від клавіатури; циклічне опитування стану клавіатури з великою швидкістю; встановлення драйвера-фільтра з метою підключення до стеку клавіатури; стеження за викликами API-функцій; використання пристроїв для непомітного запису інформації при натисканні клавіш користувачем і т.і.

Отже, величезна кількість конфіденційної інформації, яка фігурує у комп'ютерних системах, вимагає захисту взагалі і від клавіатурних шпигунів зокрема. У тих випадках, коли з'являється необхідність виявити наявність

клавіатурних шпигунів у системі, можна використати такі параметри пошуку, як:

- пошук за сигнатурами;
- застосування евристичних алгоритмів;
- здійснення моніторингу API-функцій;
- відстеження системою драйверів, процесів і сервісів.

У доповіді йдеться про один з підходів до захисту програм від кейлогерів, а саме про розробку модуля, який вбудовується у захищувані програми і спрацьовує лише при введені важливої інформації. А яка інформація є важливою, визначає розробник програмного продукту та вбудовує у свою програму певний фрагмент коду для впровадження та зняття захисту. Сутність методу захисту полягає у здійсненні моніторингу API-функцій шляхом реалізації хук-процедури, яка перехоплює усі виклики хука клавіатури, фільтрує їх, виявляє клавіатурний шпигун та блокує його роботу.

Таким чином, розробник програми самостійно вирішує, яка частина його програмного засобу є критичною і вимагає вбудовування модуля захисту. Якщо подальше виконання програми не вимагає приховування клавіатурного введення, захист знімається, про що рішення приймає також розробник. Даний захист виконано у вигляді окремих процедур, що зведені в окрему бібліотеку динамічного компонування, яку розробник програми повинен під'єднати при розробці програми.

Зручність такого захисту у тому, що він не вимагає від розробника основної програми знання принципів роботи програм-шпигунів. Але, звичайно, один лише цей метод не дає стовідсоткового захисту. Для забезпечення більш надійного захисту передбачається побудувати систему, в якій будуть поєднанні і ряд інших методів виявлення шпигунів ї захисту від них з тим, щоб вони перевіряли і доповнювали один одного.