УДК 004.[021+023]

Разработка Userspace - методов защиты ввода символов с клавиатуры.

Н.Н.Ефанов*[1], *С.А.Лебёдкин

[1]Московский физико-технический институт (государственный университет)

Рассмотрена задача перехвата данных от устройств пользовательского ввода и разработке средств защиты пространства пользователя, устойчивых к такому перехвату по построению.

Большая часть пользовательских текстовых данных вводится с различных клавиатур в виде последовательностей скан-кодов , преобразуемых на различных уровнях ОС в последовательности символов. Возникает задача защиты вводимых данных от различных «кейлоггеров» - ПО для регистрации действий пользователя через устройства ввода[1-5]. Данное ПО может использоваться для шпионажа за поведением пользователя, сбора конфиденциальной информации, либо в целях администрирования и контроля в гос. учреждениях и компаниях.

Доклад состоит из двух частей. Первая часть посвящена краткой классификации и анализу базовых методов кейлоггинга по таким показателям как механизмы внедрения, особенности реализации, сложности обнаружения и «лечения» системы после внедрения, применительно к ОС Linux. В ходе работы исследованы следующие методы:

1.Виртуализационные.

2.Уровня ядра Linux. Рассматриваются 3 актуальных метода подмены и модификации системного вызова, перехваты обработчика TTY очереди и драйвера устройства.

3.Уровня пространства пользователя Linux. Расматривается перехват событий X-сервера и перехват как кодов символов, так и самих символов, получаемых по таблице преобразования напрямую или посредством X API. Также рассматриваются такие методы как подмена библиотечного вызова посредством выставления переменной окружения LD_PRELOAD, и чтение из /dev/inputX после ioctl (EVIOCGNAME).

Большую часть кейлоггеров на базе вышеперечисленных методов, особенно виртуализационные и уровня ядра, тяжело обнаружить и обойти из пространства пользователя[5]. Ввиду вышесказанного, встаёт вопрос разработки систем защиты, устойчивых к «низкоуровневому» перехвату скан-кодов или символов. Данные методы, предлагаемые во 2-й части, по построению делают ядерные и гипервизорные перехваты

неэффективными, ввиду невозможности восстановить исходную последовательность без анализа алгоритмов работы и состояния системы.

Метод №1 - динамическая генерация раскладки клавиатуры, в соответствии с которой вводимые с клавиатуры символы переводятся в конечный текст. Зашифрованная раскладка передаётся на целевое, либо стороннее устройство и отображается на экране, либо выводится на печать.

Метод №2 – система стенографического ввода, преобразующая в соответствии с таблицей последовательности 1-4 движений мышью по 4 направлениям в символы латинской клавиатуры + спец. символы.

На базе тестирования разработанных авторами прототипов решений №1 и №2 приводятся выводы об области эффективной применимости последних, в том числе для решений на JVM и внутри изолированного Linux-контейнера.

Литература

1. *Andrew Schulman* The Extent of Systematic Monitoring of Employee E-mail and Internet Use, 2001. Электронный источник: http://www.diogenesllc.com/internetmonitoring.pdf

2. *Nikolay Grebennikov* Keyloggers: how they work and how to detect them (Part 1). Securelist, AO Kaspersky Lab, 2007. Электронный источник: https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/

3. *Nikolay Grebennikov* Keyloggers: implementing keyloggers in Windows: part two. Securelist, AO Kaspersky Lab, 2011. Электронный источник: https://securelist.com/analysis/publications/36358/keyloggers-implementing-keyloggers-in-windows-part-two/

4. Windows Internals // David Solomon, Mark Russinovich, Alex Ionescu. — Microsoft Press, 2012.

5. *Зайцев О.* Rootkits, SpyWare, AdWare, Keyloggers & BackDoors. Обнаружение и защита. — Санкт-Петербург: БХВ-Петербург, 2006.