УДК 004.492.3

ЭФФЕКТИВНОЕ ОБНАРУЖЕНИЕ ВРЕДОНОСНЫХ СИСТЕМНЫХ ВЫЗОВОВ В ПОЛЬЗОВАТЕЛЬСКОМ РЕЖИМЕ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS

Алиев А. А. (Университет ИТМО)
Научный руководитель – кандидат технических наук, Маркина Т.А.
(Университет ИТМО)

Введение. В условиях постоянно растущих киберугроз становится неотъемлемой необходимостью развивать эффективные методы обнаружения и предотвращения вредоносных атак, особенно в контексте возможности злоумышленников обходить меры защиты антивирусов, в частности путем обхода перехватов вызовов высокоуровневых API Windows с помощью системных вызовов. В рамках данной работы представлен подход к реализации перехватов системных вызовов в пользовательском режиме операционной системы Windows, основанный на применении инструментария обратных вызовов.

Основная часть. Путем использования системных вызовов злоумышленники могут уклониться от обнаружения и осуществлять атаки на систему, обходя все методы перехвата, применяемые антивирусами. Многие антивирусные программы осуществляют перехват вызовов API операционной системы Windows. Перехваты представляют собой специальные инструкции, которые позволяют антивирусам перехватывать поток управления программы при вызове определенной функции, обеспечивая контроль и отслеживание ее действий. Путем анализа вызовов можем проследить путь до библиотеки NTDLL, которая является интерфейсом между пользовательским пространством и ядром операционной системы. Изучив структуру и функционирование библиотеки в дизассемблированном виде становится ясно, что для выполнения системного вызова необходимо поместить номер соответствующей системной службы в определенный регистр, а затем осуществить вызов. Таким образом, возможно создание заглушки, позволяющей обойти перехватчики антивирусных программ и выполнять системные вызовы без их обнаружения.

В контексте пользовательского режима было предложено ограниченное количество средств для противодействия этой технике. Несмотря на то, что подобные системные вызовы можно эффективно контролировать из режима ядра, большинство систем обнаружения по различным причинам продолжают работать исключительно в пользовательском режиме.

В рамках данного исследования предлагается использование инструментария обратных вызовов для реализации перехвата системных вызовов. Этот подход не только направлен на создание эффективного средства обнаружения подобных системных вызовов, но и включает механизмы для предотвращения таких атак.

Выводы. Результаты исследования подтверждают, что предложенный метод, использующий инструментарий обратных вызовов, предоставляет эффективные средства выявления и предотвращения вредоносных системных вызовов в пользовательском режиме.

Список использованных источников:

1. Руссинович М., Соломон Д., Ионеску Алекс. Внутреннее устройство Windows. 7-е изд. // пер. с анг. – Изд-во: Издательский дом "Питер", 2018. – 944 с – ISBN 5446106636.
2. Image File Machine Constants // Microsoft [официальный сайт]. URL: https://learn.microsoft.com/en-us/windows/win32/sysinfo/image-file-machine-constants (дата обращения: 12.01.2024)
3. Red Team Tactics: Combining Direct System Calls and sRDI to bypass AV/EDR // Outflank. – URL: https://www.outflank.nl/blog/2019/06/19/red-team-tactics-combining-direct-

system-calls-and-srdi-to-bypass-av-edr/ (дата обращения: 01.02.2024)
4. Ligh M.H., Case A., Levy J., Walters A. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory Indianapolis. Wiley, 2014.
5. Direct Syscalls: A journey from high to low // REDOPS. – URL: https://redops.at/en/blog/direct-syscalls-a-journey-from-high-to-low (дата обращения: 05.01.2024)