УДК 004.056

АППАРАТНО-ПРОГРАММНЫЕ МЕХАНИЗМЫ БЛОКИРОВКИ ВРЕДОНОСНОГО КОДА

А.К. Крамаренко, А.В. Лопато
Учреждение образования «Брестский государственный технический университет», г. Брест, Республика Беларусь

Аннотация. Рассмотрены аппаратные решения на уровне процессора (NX/XD-бит, технологии изолированных сред исполнения), программные методы контроля приложений (AppLocker, Windows Defender Application Control) и интеллектуальные системы на базе репутационного анализа (Smart App Control). Также приводятся сведения о поведенческих методах обнаружения аномалий выполнения программ и динамических песочницах.
Ключевые слова: NX/XD-бит; контроль приложений; Smart App Control; доверенная среда исполнения; поведенческий анализ; динамическая песочница.

HARDWARE-SOFTWARE MECHANISMS FOR MALICIOUS CODE BLOCKING

A.K. Kramarenko, A.V. Lopato
Educational Institution "Brest State Technical University", Brest, Republic of Belarus

Abstract. Hardware solutions at the processor level (NX/XD-bit, isolated execution environment technologies), software application control methods (AppLocker, Windows Defender Application Control) and intelligent systems based on reputation analysis (Smart App Control) are considered. Also provides information about behavioral methods for detecting program execution anomalies and dynamic sandboxes.
Keywords: NX/XD-bit; application control; Smart App Control; trusted execution environment; behavioral analysis; dynamic sandboxing.

Введение

В настоящее время угрозы кибербезопасности видоизменяются, а применяемые сигнатурные методы защиты от вредоносного кода реагируют на них с задержкой. Они зачастую не своевременно реагируют на полиморфные вредоносные программы [1]. Это требует смещения применяемой защиты в сторону проактивного блокирования такой активности. В данной статье будут приведены результаты исследования некоторых аппаратно-программных комплексов защиты информации, а именно – механизмы блокировки выполнения вредоносного кода. Цель – исследование аппаратно-программных методов блокировки вредоносного кода и оценка перспективных направлений.

Основная часть

Блокировка вредоносного кода отличается от его обнаружения и лечения. Реактивные методы разрешают кратковременное выполнение

вредоносного кода до момента его обнаружения, а проактивная блокировка – предотвращение факта запуска или исполнения деструктивных инструкций. Концепция защиты строится на многоуровневом подходе (Defense in Depth) с аппаратной «песочницей» на уровне ядра. В тоже время программные надстройки управляют политиками запуска. Ключевое изменение в защите – переход от подхода «разрешено все, что не запрещено» к подходу «запрещено все, что не разрешено» [2]. В таблице представлены результаты сравнения реактивного и проактивного подходов к защите.

Сравнение реактивного и проактивного подходов к защите
Comparison of reactive and proactive approaches to protection

Характеристика	Реактивный подход (сигнатурный)	Проактивный подход (блокирование)
Принцип работы	Поиск совпадений с базой угроз	Предотвращение выполнения неизвестного кода
Время реакции	После появления сигнатуры	До запуска кода
Защита от новых угроз	Отсутствует до обновления баз	Высокая (поведенческий анализ)
Нагрузка на систему	Высокая (постоянное сканирование)	Средняя (проверка при запуске)
Ложные срабатывания	Низкие	Выше, но компенсируются настройками

Аппаратные механизмы выполняются на уровне центрального процессора. Один из основных аппаратных механизмов – это бит запрета исполнения. Он реализован в процессорах Intel (как Execute Disable Bit) и в AMD (как Enhanced Virus Protection). Суть заключается в аппаратной поддержке страничной организации памяти. Это является важным для отражения классических атак типа переполнения буфера. В случае если процессор пытается выполнить команду из области с флагом «No eXecute», он генерирует соответствующее исключение. Далее операционная система этот завершает процесс [3].

В современных операционных системах (Windows, Linux, др.) этот механизм используется совместно с программной реализацией Data Execution Prevention. Такая реализация закрывает целый класс уязвимостей, связанных с выполнением кода в неположенных сегментах памяти. Программные механизмы часто надстраиваются над аппаратными для обеспечения логики принятия решений о доверии к исполняемому коду (Control Flow Integrity или целостность потока управления). Согласно базе знаний MITRE ATT&CK, одна из эффективных контрмер – предотвращение выполнения кода через контроль приложений и блокировку скриптов. Инструменты (AppLocker, Windows Defender

Application Control, др.) разрешают администраторам задавать политики, разрешающие запуск тех исполняемых файлов, которые имеют доверенную цифровую подпись или же хранятся в определенных защищенных путях. Так блокируется выполнение «живущих с земли» бинарных файлов и скриптов [3].

Также новый виток развития – системы на базе репутационного анализа. Windows 11 Smart App Control изменяет существующую логику работы антивирусной программы. Перед запуском файла SAC обращается к облачной службе репутации Microsoft и анализирует цифровую подпись, также применяет модели машинного обучения. Если репутация файла неизвестна или он признается вредоносным, его запуск блокируется. Это решение работает проактивно.

Атаки часто направлены не на исполняемые файлы, а на скрипты (JavaScript, VBA, др.), также на цепочки поставок программного обеспечения. Патент US 9648032 описывает метод блокировки скриптов. Он основан на перехвате запроса к серверу. В области безопасной разработки появился и класс решений – Dependency Firewall (межсетевой экран для зависимостей), который изучает открытые компоненты и библиотеки до того, как они попадут в код. Это решение в реальном времени блокирует уязвимые артефакты.

Заключение

Подводя итог, отметим, что аппаратный уровень создает базу, путем разделения памяти на исполняемые и неисполняемые области и, тем самым, препятствует базовым классам атак. Программный уровень управления использует политику «белых списков» и репутационного анализа. На этом уровне запрещается запуск неподписанного или малоизвестного кода. Перспективные же методы (анализ аномалий выполнения, др.) ориентированы на блокировку неизвестных угроз и атак нулевого дня. И, совместное использование всех этих механизмов повышает степень защиты, минимизируя временной промежуток между появлением угрозы и ее блокировкой.

Список использованных источников

1. Крамаренко А. К., Русенко В. Н. (2024) Интеграция программного обеспечения в бизнес: процесс, проблемы и перспективы. Интеллектуальные ресурсы – региональному развитию. (1), 232–237.

2. Косолапов Ю. В., Павлова Т. А. (2024) Об исследовании одного способа выявления аномального выполнения программы. Моделирование и анализ информационных систем. 31 (2), 152–163.

3. Иванов М. А., Чугунков А. А. (2024) Криптографические методы защиты информации. 3-е изд., испр. и доп. Москва: Юрайт. 315 с.

References

1. Kramarenko A. K., Rusenko V. N. (2024) Integration of Software into Business: Process, Problems and Prospects. Intellectual Resources – Regional Development. (1), 232–237 (in Russian).

2. Kosolapov Yu. V., Pavlova T. A. (2024) On the Study of a Method for Detecting Anomalous Program Execution. Modeling and Analysis of Information Systems. 31 (2), 152–163 (in Russian).

3. Ivanov M. A., Chugunkov A. A. (2024) Cryptographic Methods of Information Protection. 3rd ed., corrected and supplemented. Moscow: Yurayt. 315 p. (in Russian).

Сведения об авторах

Крамаренко А.К., канд. экон. наук, доц., доц. кафедры бухгалтерского учета, анализа и аудита, учреждение образования «Брестский государственный технический университет», annnakramarenko@yandex.by.

Лопато А.В., студент факультета электронно-информационных систем, учреждение образования «Брестский государственный технический университет», artemlopato11@gmail.com.

Information about the authors

Kramarenko A.K., Cand. Sci. (Econ.), Associate Professor, Associate Professor of the Department of Accounting, Analysis, and Audit, Educational Institution "Brest State Technical University", annnakramarenko@yandex.by

Lopato A.V., student, Faculty of Electronic Information Systems, Educational Institution "Brest State Technical University", artemlopato11@gmail.com.