УДК 004.732.056

С.Ю. Гавриленко, И.В. Шевердин

Национальный технический университет «ХПИ», Харьков

УСОВЕРШЕНСТВОВАННАЯ КОНЦЕПЦИЯ ЗАЩИТЫ ДАННЫХ НА БАЗЕ МНОГОУРОВНЕВОГО АНАЛИЗА КАРТ ОПЕРАЦИОННОЙ СИСТЕМЫ

Разработана многоуровневая антивирусная система, базирующаяся на анализе системных событий и низкоуровневых команд. Архитектурно система операционно-зависима, что позволяет сформировать карты уровней конкретно выполняемой операционной системы, основываясь на различии драйверов устройств и различных системных компонентах. Анализ процессов, а не групп системных компонентов, позволяет увеличить быстродействие системы по сравнению с существующими реализациями эвристического анализа.

Ключевые слова: *компьютерные системы, антивирусные системы, анализ процессов в операционной системе, многоуровневые системы анализа данных.*

Введение

Постановка проблемы и анализ литературы. Одним из самых актуальных вопросов современной безопасности является обеспечение целостности и защиты информации [1]. Мы живем в эру развития информационной компьютерной компетенции, с каждым днем наша работа, образование и отдых трансформируется в автоматизированные сервисные решения, реализованные на базе компьютерного оборудования и соответствующего программного обеспечения. Наша жизнь становится цифровой и наравне с физической безопасностью нам необходимы средства защиты информации нашего цифрового мира.

Современные антивирусные программы позволяют не только выявлять, но и предотвращать несанкционированный доступ вредоносных программ [2, 3]. Большинство современных антивирусных программ запускается автоматически операционной системой, и постоянно проверяют безопасность осуществляемых другими программами действий, а также контролируют оперативную память и файловую систему компьютера. Но антивирусная программа не может дать достаточно высокий уровень защиты, так как она зависит от обновления и сигнатурных баз вирусов. Эта проблема частично решается эвристическим методом, но данный метод реализованный в современных антивирусных программах не дает абсолютную гарантию обнаружения из-за основных принципов работы [4, 5]. Основным минусом существующих методов эвристического анализа является большая нагрузка на выполняющую систему, ложные срабатывания, отсутствие методов адаптации и обучения.

Именно поэтому актуальной темой является разработка эффективных методов и технологий противодействия компьютерным вирусам.

Цель статьи. Разработка многоуровневой антивирусной системы формирования карт анализа процессов в операционной системе, для обнаружения вредоносного программного обеспечения.

Основная часть

В работе предложена многоуровневая антивирусная система формирования карт (MAP – Monitor Automatic Page) которая выполняет анализ процессов в операционной системе, что позволяет обнаружить все виды вирусных атак, так как для выполнения какого-либо вредоносного воздействия вирусу необходим процесс. Даже если данный вирус является набором скриптов, будут использованы интерпретаторы операционной системы, которые в свою очередь также являются процессами.

Предложенная система не зависит от большого объёма сигнатурных баз, обладает быстрым временем обнаружения вредоносного операционного процесса и выполнена в виде отдельного модуля специального назначения для антивирусных программ.

Архитектурно данная система является операционно-зависимой. Это обеспечивает формирование карт уровней для конкретно выполняемой операционной системы, основываясь на различии драйверов устройств и различных системных компонентах.

Для построения карточного анализа используется многоуровневая система анализа поведения состояний операционной системы (рис. 1). Основной принцип работы данной системы – это формирование карт уровней 0 и 1, а также выполнение анализа посредством второго уровня для проверки инструкций процесса. В качестве механизма сопоставления карт используется метод нечеткой логики, позволяющий сделать вывод о возможности вредоносного воздействия данного процесса на систему.

Карты уровня 0 – это карты аппаратного уровня, которые описывают систему в целом, а именно реестр, оперативную память, дисковое пространство, поток интернет пакетов. Карты уровня 1 – это карты уровня процессов, которые описывают поведение процесса, а именно выполнение операций с дисковым пространством, изменение реестра, взаимодействие с сетевыми ресурсами, формирование новых потоков и коммуни-

кация со сторонними процессами. Карты уровня 2 – это карты низкоуровневого анализа инструкций процесса, представляющие собой команды языка ассемблера. Карты содержат последовательность вредоносных команд.

Для повторного анализа существующих карт каждого уровня применяется два механизма: ретроспектива для уровня 1 и интроспектива для уровня 2. Ретроспектива карт – это повторный анализ состояния процессов уровня 1 с построением дерева карт, используя уровень 2.

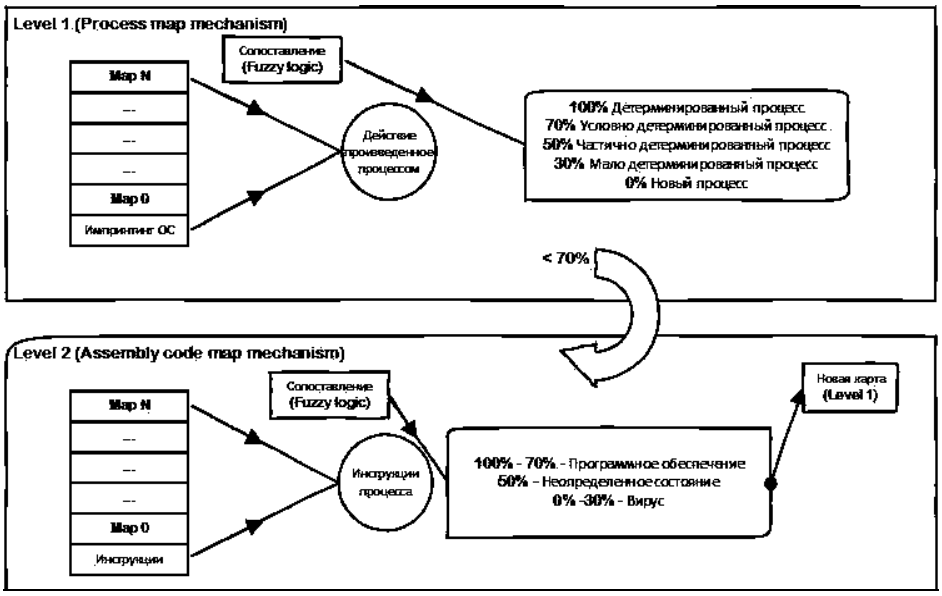

Рис. 1. Многоуровневая антивирусная система формирования карт

Дерево карт – это специализированная структура данных, которая агрегирует ряд состояний процесса до 10-го поколения и связывает системные события с процессами, которые породили данное событие. Интроспектива карт – это анализ низкоуровневых вредоносных команд для карт уровня 2, путем формирования зависимостей между существующими командами. Ретроспектива проводится в случае простоя компьютерного оборудования.

Карты для уровня 1 создаются после функционального исследования процессорных команд на уровне 2. Карты для уровня 2 формируются оператором антивирусной системы и являются перманентной частью системы, агрегирующей ряд инструкций языка ассемблера согласно критерию опасности команд, что позволяет в дальнейшем, используя данный ряд инструкций выполнить интроспективу карт и скорректировать карты. Так как большинство информации, получаемой из системных событий представляет собой строковый набор данных, то карты уровней представляются в виде хеш-таблиц. Для быстрого поиска в ней используется алгоритм Рабина-Карпа, что позволяет находить и сопоставлять информацию за асимптотически минимальное время.

Многоуровневый подход позволяет получить минимальное количество ложных срабатываний, путем анализа всех системных событий в целом, а не определенного набора команд процессов. Современные антивирусы анализируют определенный ряд команд процессов и при наличии последовательности вредоносных команды блокируют вызывающий процесс. Предложенный метод анализирует все события операционной системы, что повышает вероятность обнаружения вирусной активности. Для предотвращения ложного определения реализованы дополнительные уровни анализа, это уровень 0 и 2, что позволяет анализировать не только события, но и содержимое памяти, реестра, интернет пакетов на уровне 0, а уровень 2, соответственно позволяет провести анализ системных команд процессов в момент поступления события на уровне 1. Таким образом достигается полная информационная консистентность статистических данных, формирующих карты операционной системы.

Результаты разработки и исследований основных этапов работы MAP. MAP инсталлируется после установки операционной системы семейства Windows 7/8/8.1/10 и выполняет формирование первоначальных карт уровня 1 операционной системы, описывая все процессы в системы (импринтинг операционной системы). После установки нового программного обеспечения MAP запускает механизм сопоставления карт, который укажет наличие новых процессов в системе, и выполнит переход на уровень 2 для определения новых инструкции в процессе. Полученный набор новых инструкций подвергается анализу, используя аппарат нечеткой логики и определяется наличие вредоносных команд в данном процессе (рис. 2). После чего формируется новая карта для уровня 1. Так как точность в данный момент может варьироваться от 0% или 100% MAP, то необходимо сформировать список интроспективного анализа и занести процессы в очередь.

При повторении процессов, есть вероятность изменения статистики путем добавления новых состояний в виде карт, что может привести в дальнейшем к переходу от неопределенного состояния к определению процесса как программного компонента или вируса (пузырек интроспекции). Если система не задействует свои ресурсы, то MAP выполнит ретроспективу. Пользователь также будет статистически описан системой MAP с помощью механизма, который формирует специфическую карту зеркально насыщенного нейронного повторения. Карта зеркально насыщенного нейронного повторения представляет собой статистически построенную карту выполнения

пользователем перманентных действий в системе, которые формируют пользовательское (административное) состояние системы, описанное нейронной сетью в течение недели работы операционной системы. Результаты показали целесообразность использования карт и алгоритмических механизмов для обнаружения вредоносного программного обеспечения.

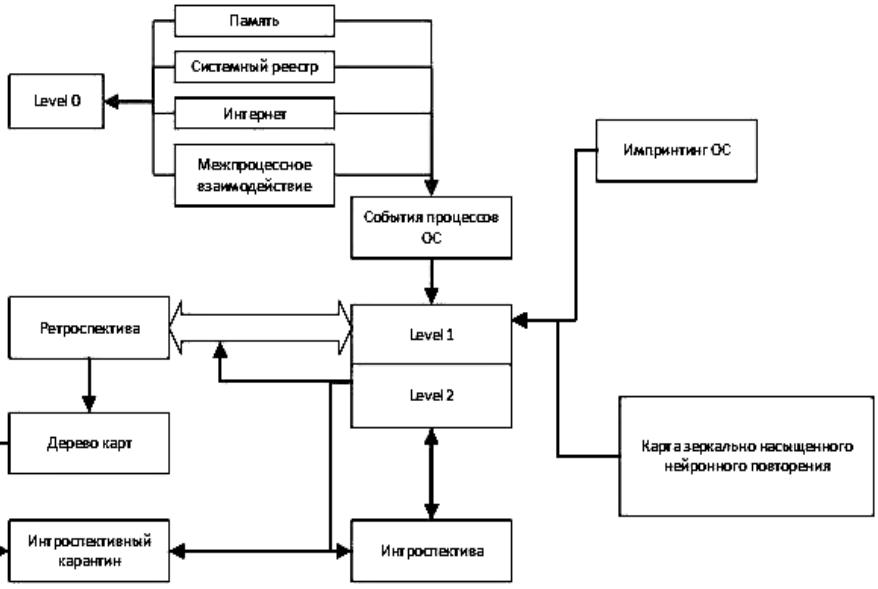

Рис. 2. Структурная схема антивирусной системы защиты данных на базе многоуровневого анализа карт операционной системы

Выводы

В работе впервые предложена многоуровневая антивирусная система формирования карт анализа процессов в операционной системе для обнаружения вредоносного программного обеспечения. Анализ процессов, а не групп системных компонентов, позволяет увеличить быстродействие системы по сравнению с существующими реализациями эвристического анализа. Для быстрого анализа и сопоставления результатов различных карт на всех уровнях MAP используются хеш-таблицы. Максимально возможное предотвращение ложных срабатываний, достигается путем внедрения многоуровневой системы анализа, компенсирующей и формирующей статистический ряд по масштабно ориентированному набору, а именно система анализируется глобально, оцениваются масштабные изменения, изменения событий процессов системы, а также низкоуровневые системные команды. Отсутствие методов адаптации и обучения решается путем внедрения новых карт во все уровни путем обучения, каждый уровень способен создать карту для предыдущего уровня.

Список литературы

1. *The best antivirus protection of 2017 [Електронний ресурс] – Режим доступу: http://uk.pcmag.com/antivirus-reviews/8141/guide/the-best-antivirus-protection-of-2017.*

2. *Касперський К. Записки дослідника комп'ютерних вірусів. / К. Касперський. - СПб .: Пітер, 2006. - 316 с.*

3. *Semenov. S.G. and Davydov V.V. and S.Y. Gavrilenko (2014), Data protection in computerized control systems, Ed. «LAP LAMBERT ACADEMIC PUBLISHING» Germany, 236 p.*

4. *Кнут Е. Д. Мистецтво програмування. Том 1. Основні алгоритми. М .: Видавничий дім «Вільямс», 2000. - 832 с.*

5. *Bart Kosko (1986). "Fuzzy Cognitive Maps". International Journal of Man-Machine Studies, 1986.– cc. 65–75.*

Надійшла до редколегії 31.01.2017

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

УДОСКОНАЛЕНА КОНЦЕПЦІЯ ЗАХИСТУ ДАНИХ НА БАЗІ БАГАТОРІВНЕВИХ АНАЛІЗУ КАРТ ОПЕРАЦІЙНОЇ СИСТЕМИ

С.Ю. Гавриленко, І.В. Шевердін

У статті розроблена багаторівнева антивірусна система, що базується на аналізі системних подій і низькорівневих команд. Архітектурно дана система є операційно-залежною. що дозволяє сформувати карти рівнів конкретно виконуваної операційної системи, ґрунтуючись на відмінності драйверів пристроїв і різних системних компонентах. Аналіз процесів, а не груп системних компонентів, дозволяє збільшити швидкодію системи в порівнянні з існуючими реалізаціями евристичного аналізу.

Ключові слова: *комп'ютерні системи, антивірусні системи, аналіз процесів в операційній системі, багаторівневі системи аналізу даних.*

IMPROVED DATA PROTECTION CONCEPT ON THE BASIS OF MULTI-LEVEL ANALYSIS OF THE OPERATING SYSTEM CARD

S.Yu. Gavrilenko, I.V. Sheverdine

The article developed a multi-level antivirus system, based on the analysis of system events and low-level commands. Architecturally, this system is operationally dependent. Which allows you to create maps of the levels of a specific operating system, based on the differences between device drivers and various system components. Analysis of processes, rather than groups of system components, allows to increase the speed of the system in comparison with existing implementations of heuristic analysis.

Keywords: *computer systems, anti-virus systems, analysis of processes in the operating system, multi-level systems for data analysis.*