

ОПРЕДЕЛЕНИЕ ВРЕДНОСНОЙ АКТИВНОСТИ ПО АНАЛИЗУ ПОВЕДЕНИЯ ОБЪЕКТОВ В НЕИЗОЛИРОВАННОЙ СРЕДЕ

ОБЛАСТЬ ТЕХНИКИ

- 5 Настоящее техническое решение относится к области вычислительной техники, в частности, к компьютерно-реализуемому способу и системе определения вредоносной активности по анализу поведения объектов в неизолированной среде.

УРОВЕНЬ ТЕХНИКИ

- 10 Из источника информации RU 2 451 326 C2, 20.05.2012, известен способ системного анализа и управления, который осуществляется при помощи системы, которая включает в себя одну или более компьютерных программ или агентов, которые сообщают данные, связанные с происходящими внутри системы модификациями. Эти данные включают в себя информацию, связанную со всеми взаимодействиями с файлами и/или настройками. Подобные типы
- 15 взаимодействий включают в себя такие действия, как чтение или запись в элементы системного реестра, файлы, а также взаимодействия бинарного модуля, такие как загрузка и т.д. Агенты сообщают собранные данные в серверную службу, которая обрабатывает полученную информацию для, например, генерации веб-отчетов, предупреждений или для интегрирования с другими службами в целях выполнения управления системой.
- 20 Из источника информации US 9,245,114 B2, 26.01.2016, известен способ для автоматического обнаружения и анализа вредоносных программ, который включает следующие шаги: сохранение системой анализа базовой линии памяти для первой системы, базовой линии памяти, включающей в себя информацию, хранящуюся в энергозависимой памяти первой системы, и энергонезависимой памяти первой системы, предоставление системой анализа файла в первую
- 25 систему, выполнение системой анализа файла в первой системе с использованием операционной системы первой системы после сохранения базовой линии памяти, завершение системой анализа работы операционной системы первой системы после выполнения файла, сохранение системой анализа карты памяти после выполнения первой системы, в то время как работа операционной системы первой системы завершается, карта памяти после выполнения включает в себя
- 30 информацию, хранящуюся в энергозависимой памяти первой системы, и - энергозависимая память первой системы после выполнения файла. Способ также включает анализ с помощью системы анализа базовой линии памяти и карты памяти после выполнения, причем анализ содержит: определение наличия одного или нескольких процессов, которые изменились с базовой линии памяти на карту памяти после выполнения, определение временных отметок, связанных с одним
- 35 или несколькими процессами, и выявление поведения, которое указывает на попытки скрыть руткит во время работы операционной системы; определение того, что файл содержит вредоносное программное обеспечение, на основе анализа; определение сроков действий, выполняемых вредоносным программным обеспечением, на основе меток времени; и предоставление отчета о

вредоносном программном обеспечении, включая список одного или нескольких процессов, которые изменились, и временную шкалу.

Предлагаемое решение отличается от известных из уровня техники решений тем, что информацию о работе хоста собирают в поток событий, который передают в вычислительное устройство и по меньшей мере одно событие из потока событий в зависимости от типа поступает на по меньшей мере один адаптер, при этом по меньшей мере один адаптер генерирует свое внутреннее событие. Кроме того, сгенерированные внутренние события подают в блок сигнатур, где осуществляют проверку внутреннего события по заранее заданным правилам, и в случае соответствия внутреннего события заранее заданным правилам создают маркер внутреннего состояния. Стоит отметить, что решение о вредоносной активности принимают посредством блока принятия решений на основе маркеров внутренних состояний блока сигнатур: по сумме весов маркеров внутренних состояний или вероятности вредоносности маркера внутреннего состояния или определения вредоносной активности на основе отличия от разрешенного поведения.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Технической проблемой, на решение которой направлено заявленное решение, является создание компьютерно-реализуемого способа и системы определения вредоносной активности по анализу поведения объектов в неизолированной среде, которые охарактеризованы в независимых пунктах формулы. Дополнительные варианты реализации настоящего изобретения представлены в зависимых пунктах изобретения.

Технический результат заключается в определении вредоносной активности по анализу поведения объектов в неизолированной среде.

Заявленный результат достигается за счет осуществления компьютерно-реализуемого способа определения вредоносной активности по анализу поведения объектов в неизолированной среде, включает этапы, на которых:

посредством блока обнаружения собирают информацию по меньшей мере в один поток событий;

передают на вычислительное устройство по меньшей мере один поток событий, где осуществляют анализ полученного потока событий за заранее заданное время, при этом

по меньшей мере одно событие из потока событий отправляют на вход по меньшей мере одному конечному автомату, в зависимости от типа события;

по меньшей мере одно событие из потока событий отправляют на вход по меньшей мере одному адаптеру в зависимости от типа события, причем по меньшей мере один адаптер генерирует свое внутреннее событие;

по меньшей мере одно внутреннее событие подают в по меньшей мере один блок сигнатур, где осуществляют проверку полученного по меньшей мере одного внутреннего события заранее заданным правилам и в случае соответствия по меньшей мере одного внутреннего события заранее заданным правилам создают по меньшей мере один маркер внутреннего состояния;

по меньшей мере один маркер внутреннего состояния отправляют на вход блока принятия решений о вредоносной активности, при этом если маркер внутреннего состояния с суммой весов или вероятность вредоносности маркера внутреннего состояния больше заранее заданного значения, вредоносная активность присутствует или вредоносная активность определяется на
5 основе отличия от разрешенного поведения;

составляют отчет по подозрительной активности.

В частном варианте реализации предлагаемого способа, по меньшей мере одно внутреннее событие поступает на вход конвейера, в котором сохраняется информация, которую в дальнейшем может использовать блок сигнатур.

10 В другом частном варианте реализации предлагаемого способа, по меньшей мере один маркер создается на основе обнаружения вредоносной активности или объекта в сети или на конечном узле.

В другом частном варианте реализации предлагаемого способа, по меньшей мере один маркер имеет время жизни.

15 В другом частном варианте реализации предлагаемого способа, все маркеры имеют разный вес.

В другом частном варианте реализации предлагаемого способа, внутреннее состояние состоит по меньшей мере из набора флагов, путей файлов, реестра, процессов, подписей, мьютексов, объектов синхронизации, счетчиков.

20 В другом частном варианте реализации предлагаемого способа, внутреннее состояние имеет время жизни.

В другом частном варианте реализации предлагаемого способа, блок принятия решений выполнен по меньшей мере в качестве линейной модели, обученного классификатора или нейронной сети.

25 В другом частном варианте реализации предлагаемого способа, отчет о вредоносной активности содержит, по меньшей мере маркеры сигнатур, вердикт блока принятия решений, информацию по хосту, содержимое переменных окружения, информацию о подключенных устройствах, снимок экрана, видео с экрана за момент детектирования, последовательность действий пользователя, граф инцидента.

30 Заявленный результат также достигается за счет системы определения вредоносной активности по анализу поведения объектов в неизолированной среде содержащей:

блок обнаружения, установленный на хосте и выполненный с возможностью сбора информации о по меньшей мере одном потоке событий и передачи по меньшей мере одного потока событий на вычислительное устройство;

35 вычислительное устройство, выполненное с возможностью осуществления определения вредоносной активности по анализу поведения объектов в неизолированной среде;

блок создания отчета.

ОПИСАНИЕ ЧЕРТЕЖЕЙ

Реализация изобретения будет описана в дальнейшем в соответствии с прилагаемыми чертежами, которые представлены для пояснения сути изобретения и никоим образом не ограничивают область изобретения. К заявке прилагаются следующие чертежи:

5 Фиг.1, иллюстрирует систему определения вредоносной активности по анализу поведения объектов в неизолированной среде.

 Фиг.2, иллюстрирует компьютерно-реализуемый способ определения вредоносной активности по анализу поведения объектов в неизолированной среде.

 Фиг. 3, иллюстрирует пример общей схемы вычислительного устройства.

10

ДЕТАЛЬНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

В приведенном ниже подробном описании реализации изобретения приведены многочисленные детали реализации, призванные обеспечить отчетливое понимание настоящего изобретения. Однако, квалифицированному в предметной области специалисту, будет очевидно

15 каким образом можно использовать настоящее изобретение, как с данными деталями реализации, так и без них. В других случаях хорошо известные методы, процедуры и компоненты не были описаны подробно, чтобы не затруднять излишне понимание особенностей настоящего изобретения.

Кроме того, из приведенного изложения будет ясно, что изобретение не ограничивается

20 приведенной реализацией. Многочисленные возможные модификации, изменения, вариации и замены, сохраняющие суть и форму настоящего изобретения, будут очевидными для квалифицированных в предметной области специалистов.

Заявленный компьютерно-реализуемый способ определения вредоносной активности по анализу поведения объектов в неизолированной среде осуществляется посредством системы

25 определения вредоносной активности по анализу поведения объектов в неизолированной среде (10), которая представлена на Фиг.1 и содержит:

 блок обнаружения (S10), установленный на хосте и выполненный с возможностью сбора информации о по меньшей мере одном потоке событий и передачи по меньшей мере одного потока событий на вычислительное устройство;

30 вычислительное устройство (S20), выполненное с возможностью осуществления способа определения вредоносной активности по анализу поведения объектов в неизолированной среде;

 блок создания отчета (S30).

Стоит также отметить, что описываемая система 10 полностью масштабируема, а именно может работать как в локальной, так и в глобальной сети.

35 Как представлено на Фиг. 2, заявленный компьютерно-реализуемый способ определения вредоносной активности по анализу поведения объектов в неизолированной среде (100) реализован следующим образом.

На хостах размещают программные средства сбора данных, например, блоки обнаружения событий безопасности или мониторы событий безопасности, которые занимаются ведением логов и фиксацией подозрительных событий в сети.

Стоит отметить, что в материалах настоящей заявки, под хостом понимается узел сети.

5 Хостами могут быть как физические устройства — компьютеры, серверы, ноутбуки, смартфоны, планшеты, игровые приставки, телевизоры, принтеры, сетевые концентраторы, коммутаторы, роутеры, произвольные устройства, объединённые IoT («интернетом вещей») и т.п., так и программно-аппаратные решения, позволяющие организовать несколько узлов сети на одном физическом устройстве.

10 На этапе 110, посредством блока обнаружения (S10), собирают информацию по меньшей мере в один поток событий. Так, в поток событий собирают заранее определённый набор информации о работе хоста.

Стоит отметить, что поток событий содержит по меньшей мере одно событие, например, создание файла, удаление файла, переименование файла, создание ключа реестра, запись значений в реестр, удаление значений из реестра, удаление ключа реестра, создание и завершение процесса, создание и завершение потока процесса (thread), событие лога, создание объекта ядра, и так далее, но не ограничиваясь этим списком.

15 Готовый поток событий на этапе 111 передают на вычислительное устройство (S20), где происходит анализ полученного потока за заранее заданное время. Помимо потока событий, на вычислительное устройство также может передаваться дополнительная информация, которая поступает параллельно с потоком событий. В качестве примера такой информации может выступать вердикт «песочницы» о находящихся в ней файлах или видео с экрана хоста, если таковой оборудован экраном, и другая информация.

Стоит отметить, что изначально все события в потоке событий не являются доверенными.

25 Таким образом, полученный вычислительным устройством (S20) от расположенных на хостах мониторов сырой поток событий сохраняют в памяти.

Далее по меньшей мере одно событие из списка событий собирается в массив событий, и затем, на этапе 115, по меньшей мере одно событие поступает на вход по меньшей мере одного адаптера, в зависимости от определенного типа событий.

30 После того, как на вход адаптера поступило событие, адаптер генерирует свое внутреннее событие. Таким образом обеспечивается поддержка разных форматов входных событий, то есть инвариантность событий для конвейеров и сигнатур.

Полученный массив внутренних событий на этапе 120 поступает на вход конвейера, в котором сохраняется информация, которую в дальнейшем может использовать блок сигнатур.

35 В материалах настоящей заявки конвейер осуществляет только хранение информации, полученной на этапе 111. Так, конвейер может быть выполнен в виде дерева процессов, но не ограничиваясь.

В частности, если на вход конвейера поступает внутреннее событие — ProcessCreated #1, то конвейер, получив такое внутреннее событие, сохраняет себе информацию о процессе в дереве процессов. Кроме того, в конвейерах может сохраняться информация, которая поступала на этапе 111 на вычислительное устройство, например, вердикт «песочницы» о файлах, видео с экрана и другая информация.

На этапе 121 внутреннее событие поступает в блок сигнатур, где проверяется на соответствие определенным, заранее заданным, правилам и в случае соответствия внутреннего события определенным правилам создается маркер внутреннего состояния.

В материалах настоящей заявки под блоком сигнатур понимается сущность, которая в случае соответствия внутреннего события определенным правилам создает маркер, а под правилом понимается, правило, способное отобрать в базе данных известной структуры те вхождения, которые удовлетворяют заданным условиям.

Так например, рассмотрим сигнатуру `wer_dump` и внутреннее событие ProcessCreated #2. В данном конкретном случае блок сигнатур, получив внутреннее событие, производит проверку на соответствие внутреннего события правилу, далее находит в дереве процессов процесс, который неудачно завершился, и создает маркер внутреннего состояния - «процесс неудачно завершился».

Кроме того, стоит отметить, что блок сигнатур выполнен с возможностью использования дополнительной информации конвейера, которая поступала на этапах 115-120 и дополнения ей созданные маркеры.

Таким образом, на этапе 121 по меньшей мере один блок сигнатур получает событие и сохраняет свое внутреннее состояние и внутренние данные. В качестве примера, блок сигнатур сохраняет значение `BootTime` с целью определения времени перезагрузки компьютера, а также создаёт маркер внутреннего состояния, который в сочетании с другими маркерами внутренних состояний может свидетельствовать о вредоносной активности и/или вредоносном объекте, обнаруженных в сети, либо на хосте. Соответственно, если такой информации не обнаружено, то маркер внутреннего состояния не создают.

Стоит отметить, что внутреннее состояние может состоять из по меньшей мере набора флагов, путей файлов, реестра, процессов, их подписей, мьютексов, событий (объектов синхронизации), сетевых взаимодействий, а также различных счетчиков. Также внутреннее состояние имеет определённое время жизни, которое может быть как бесконечным, так и конечным, наперёд заданной длительности.

Так, каждый маркер внутреннего состояния имеет свой вес и заранее заданное время жизни. Кроме того, время жизни устанавливают по результатам тестовых исследований на срабатывание маркера, так при выявлении вредоносной активности определяют периоды, в которых было отмечено минимальное количество ошибок первого и второго рода.

Под ошибкой первого рода подразумевается ситуация, в которой отвергнута правильная нулевая гипотеза. Например, срабатывание маркера на безвредную активность.

Под ошибкой второго рода — ситуация, в которой принята неправильная нулевая гипотеза. Например, маркер не сработал на вредоносную активность либо объект.

Дополнительно, вся информация, которая сохраняется блоком сигнатур, поступает в средство хранения данных, с указанием времени жизни этой информации. При этом, информация удаляется, если истекло ее время жизни, и внутреннее состояние конечного автомата (которым является блок сигнатур) изменяется. В некоторых случаях при изменении внутреннего состояния также может дополнительно создаваться определённый маркер.

На этапе 122 на блок принятия решений подается массив маркеров внутренних состояний от блока сигнатур, на основании которого определяется, присутствует вредоносная активность и/или вредоносный объект или нет.

В качестве блока принятия решений могут использоваться, по меньшей мере, линейная модель или классификатор. (например, Random Forest или SVM, или нейронная сеть).

В первом случае, если в качестве блока принятия решений используется линейная модель, а в определенном окне времени есть маркеры внутренних состояний с суммой весов больше порогового значения, то системой принимается решение о вредоносной активности объекта с вышеупомянутыми маркерами внутренних состояний.

В другом случае, если в качестве блока принятия решений используется классификатор, обученный ранее по вышеописанным этапам способа и который принимает в качестве признаков маркеры внутренних состояний, то при получении вероятности, более 50% системой принимается решение о вредоносной активности объекта с вышеупомянутыми маркерами внутренних состояний. Стоит отметить, что в качестве признаков могут быть не только маркеры внутренних состояний, а также, в дополнение, любая информация из контекста, дополнительная информация из конвейера, например, дерево процессов, счетчики производительности и т.п.

В качестве еще одного варианта блок принятия решений может быть выполнен в качестве заранее обученной системы, где конечные автоматы, которые соответствуют требованиям поведения запоминаются, а затем определяется вредоносная активность на основе отличий от советующих требованиям поведения.

На этапе 123 составляют отчет о подозрительной активности, посредством модуля создания отчета. Блок создания отчета может выводить готовый отчет, например, на диск, в базу данных, в syslog и др.

Отчет может содержать по меньшей мере маркеры внутренних состояний, вердикт блока принятия решений, дерево процессов, имя хоста, содержимое переменных окружения, информацию о подключенных устройствах, снимок экрана, видео с экрана за момент детектирования, последовательность действий пользователя, граф инцидента (процесс, инициирующий инцидент со связями-взаимодействиями, созданными файлами, созданными сетевыми соединениями и т.п.).

Кроме того, альтернативно блок создания отчетов может не создавать отчет, но сохранять в средстве хранения данных информацию по каждому маркеру, например, для дальнейшего подсчёта статистики.

На Фиг.3 далее будет представлена общая схема вычислительного устройства (300), обеспечивающего обработку данных, необходимую для реализации заявленного решения.

В общем случае устройство (300) содержит такие компоненты, как: один или более процессоров (301), по меньшей мере одну память (302), средство хранения данных (303), интерфейсы ввода/вывода (304), средство В/В (305), средства сетевого взаимодействия (306).

Процессор (301) устройства выполняет основные вычислительные операции, необходимые для функционирования устройства (300) или функциональности одного или более его компонентов. Процессор (301) исполняет необходимые машиночитаемые команды, содержащиеся в оперативной памяти (302).

Память (302), как правило, выполнена в виде ОЗУ и содержит необходимую программную логику, обеспечивающую требуемый функционал.

Средство хранения данных (303) может выполняться в виде HDD, SSD дисков, рейд массива, сетевого хранилища, флэш-памяти, оптических накопителей информации (CD, DVD, MD, Blue-Ray дисков) и т.п. Средство (303) позволяет выполнять долгосрочное хранение различного вида информации, например, вышеупомянутых файлов с наборами данных, полученных с разных хостов базы данных, содержащих записи зафиксированные в разные периоды для каждого пользователя временных интервалов, идентификаторов пользователей и т.п.

Интерфейсы (304) представляют собой стандартные средства для подключения и работы с серверной частью, например, USB, RS232, RJ45, LPT, COM, HDMI, PS/2, Lightning, FireWire и т.п.

Выбор интерфейсов (304) зависит от конкретного исполнения устройства (300), которое может представлять собой персональный компьютер, мейнфрейм, серверный кластер, тонкий клиент, смартфон, ноутбук и т.п.

В качестве средств В/В данных (305) могут использоваться: клавиатура джойстик, дисплей (сенсорный дисплей), проектор, тачпад, манипулятор мышь, трекбол, световое перо, динамики, микрофон и т.п.

Средства сетевого взаимодействия (306) выбираются из устройства, обеспечивающий сетевой прием и передачу данных, и могут представлять собой, например, Ethernet карту, WLAN/Wi-Fi модуль, Bluetooth модуль, BLE модуль, NFC модуль, IrDa, RFID модуль, GSM модем и т.п. С помощью средств (306) обеспечивается организация обмена данными по проводному или беспроводному каналу передачи данных, например, WAN, PAN, ЛВС (LAN), Интранет, Интернет, WLAN, WMAN или GSM.

Компоненты устройства (300) сопряжены посредством общей шины передачи данных (310).

В настоящих материалах заявки было представлено предпочтительное раскрытие осуществление заявленного технического решения, которое не должно использоваться как ограничивающее иные, частные воплощения его реализации, которые не выходят за рамки

испрашиваемого объема правовой охраны и являются очевидными для специалистов в соответствующей области техники.

5

10

15

20

25

30

35

Формула

1. Компьютерно-реализуемый способ определения вредоносной активности по анализу поведения объектов в неизолированной среде, включает этапы, на которых:

посредством блока обнаружения собирают информацию по меньшей мере в один поток

5 событий;

передают на вычислительное устройство по меньшей мере один поток событий, где осуществляют анализ полученного потока событий за заранее определенное количество времени, при этом

10 по меньшей мере одно событие из потока событий отправляют на вход по меньшей мере одному адаптеру в зависимости от типа события, причем по меньшей мере один адаптер генерирует свое внутреннее событие;

по меньшей мере одно внутреннее событие подают в по меньшей мере один блок сигнатур где осуществляют проверку полученного по меньшей мере одного внутреннего события заранее заданным правилам и в случае соответствия по меньшей мере одного внутреннего события

15 заранее заданным правилам создают по меньшей мере один маркер внутреннего состояния;

по меньшей мере один маркер внутреннего состояния отправляют на вход блока принятия решений о вредоносной активности, при этом если маркер внутреннего состояния с суммой весов или вероятность вредоносности маркера внутреннего состояния больше заранее заданного значения, вредоносная активность присутствует или определение блоком принятия решений

20 вредоносной активности на основе отличия от разрешенного поведения;

составляют отчет по подозрительной активности.

2. Способ по п.1, отличающийся тем, что по меньшей мере одно внутреннее событие поступает на вход конвейера, в котором сохраняется информация, которую в дальнейшем может использовать блок сигнатур.

25 3. Способ по п.1, отличающийся тем, что по меньшей мере один маркер создается на основе обнаружения вредоносной активности или объекта в сети или на конечном узле.

4. Способ по п.3, отличающийся тем, что по меньшей мере один маркер имеет время жизни.

5. Способ по п.3, отличающийся тем, что все маркеры имеют разный вес.

30 6. Способ по п.1, отличающийся тем, что внутреннее состояние состоит по меньшей мере из набора флагов, путей файлов, реестра, процессов, подписей, мьютексов, объектов синхронизации, счетчиков.

7. Способ по п.6, отличающийся тем, что внутреннее состояние имеет время жизни.

8. Способ по п.1, отличающийся тем, что блок принятия решений выполнен по меньшей мере в качестве линейной модели, обученного классификатора или нейронной сети.

9. Способ по п.1, отличающийся тем, что отчет о вредоносной активности содержит, по меньшей мере маркеры сигнатур, вердикт блока принятия решений, информацию по хосту, содержимое переменных окружения, информацию о подключенных устройствах, снимок экрана,

видео с экрана за момент детектирования, последовательность действий пользователя, граф инцидента.

10. Система определения вредоносной активности по анализу поведения объектов в неизолированной среде содержит:

5 блок обнаружения, установленный на хосте и выполненный с возможностью сбора информации о по меньшей мере одном потоке событий и передачи по меньшей мере одного потока событий на вычислительное устройство;

 вычислительное устройство, выполненное с возможностью осуществления способа определения вредоносной активности по анализу поведения объектов в неизолированной среде

10 по пп.1-9;

 блок создания отчета.

15

20

25

30

35