

СПОСОБ И СИСТЕМА ПОИСКА СХОЖИХ ВРЕДОНОСНЫХ ПРОГРАММ ПО РЕЗУЛЬТАТАМ ИХ ДИНАМИЧЕСКОГО АНАЛИЗА

5 ОБЛАСТЬ ТЕХНИКИ

Настоящее техническое решение относится к области вычислительной техники, в частности, к способу и системе поиска схожих вредоносных программ по результатам их динамического анализа.

10 УРОВЕНЬ ТЕХНИКИ

Из уровня техники известен источник информации US 9,165,142 B1, 20.10.2015, раскрывающий методы идентификации семейства вредоносных программ с использованием сигнатур профиля. В некоторых вариантах осуществления идентификация вредоносного программного обеспечения с использованием сигнатур профиля включает в себя выполнение образца потенциального вредоносного программного обеспечения в среде виртуальной машины (например, в изолированной программной среде) и определение, связан ли образец потенциального вредоносного программного обеспечения с известным семейством вредоносных программ на основе сигнатуры профиля. В некоторых вариантах осуществления, среда виртуальной машины представляет собой инструментальную среду виртуальной машины для мониторинга потенциальных образцов вредоносного программного обеспечения во время выполнения.

Из уровня техники также известен источник информации US 2019/0158525 A1, 23.05.2019, раскрывающий способы автоматической группировки вредоносных программ на основе артефактов. В некоторых вариантах осуществления системный, процессный и / или компьютерный программный продукт для автоматической группировки вредоносных программ на основе артефактов включает в себя прием множества выборок для выполнения автоматического анализа вредоносных программ для генерации файлов журнала на основе автоматического анализа вредоносных программ; обработка файлов журнала для извлечения функций, связанных с вредоносными программами; кластеризация множества выборок на основе извлеченных признаков; и выполнение действия на основе результатов кластеризации.

Предлагаемое решение отличается от известных из уровня техники решений тем, что предложенный способ, включает фиксацию действий, которые выполняются вредоносной программой, в поведенческий отчет формата JSON. Полученные отчеты разделяют таким образом, что в одной группе находятся отчеты, содержащие схожие действия и

относящиеся к одному известному вредоносному семейству. Дополнительно, стоит отметить, что в заявленном решении использован ансамбль классификаторов, который служит для повышения эффективности поиска схожих вредоносных программ по сравнению с отдельными классификаторами, а также является менее громоздким
5 решением, чем нейронная сеть.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Технической проблемой, на решение которой направлено заявленное техническое решение, является создание компьютерно-реализуемого способа и системы поиска схожих
10 вредоносных программ по результатам их динамического анализа, которые охарактеризованы в независимых пунктах формулы. Дополнительные варианты реализации настоящего изобретения представлены в зависимых пунктах изобретения.

Технический результат заключается в осуществлении поиска схожих вредоносных программ и в повышении точности отнесения вредоносных программ к известному
15 семейству вредоносных программ.

Заявленный результат достигается за счет осуществления компьютерно-реализуемого способа поиска схожих вредоносных программ по результатам их динамического анализа, который содержит:

подготовительный этап, на котором:
20 в изолированной среде анализируют по меньшей мере одну вредоносную программу;

фиксируют выполняемые по меньшей мере одной вредоносной программой действия в, по меньшей мере, одном поведенческом отчете;

разделяют накопленные поведенческие отчеты таким образом, что в по меньшей
25 мере одной группе находятся отчеты, содержащие похожие действия и/или относящиеся к одному известному вредоносному семейству;

по выбранным полям поведенческого отчета создается вектор признаков по данному известному вредоносному семейству;

на основе каждого из полученных векторов признаков обучается по меньшей мере
30 один бинарный классификатор;

создают ансамбль бинарных классификаторов на основе ранее обученных бинарных классификаторов;

рабочий этап, на котором:

анализируют по меньшей мере одну вредоносную программу;

фиксируют выполняемые по меньшей мере одной вредоносной программой действия в, по меньшей мере, одном поведенческом отчете;

запускают обученный на подготовительном этапе, ансамбль бинарных классификаторов;

- 5 ансамбль бинарных классификаторов формирует итоговую оценку, что анализируемая вредоносная программа принадлежит к по меньшей мере одному известному семейству вредоносных программ.

В частном варианте реализации описываемого способа, при анализе вредоносных программ в изолированной среде фиксируют по меньшей мере следующее:

- 10 процессы, запускаемые программой, параметры запуска каждого процесса;
файлы, создаваемые каждым процессом;
мьютексы, создаваемые каждым процессом;
ключи реестра, создаваемые каждым процессом;
запись видео с экрана виртуальной машины во время работы вредоносной
15 программы;
сетевая активность;
маркеры вредоносности.

- В другом частном варианте реализации описываемого способа, в котором отчет представляет собой отчет в формате JSON, содержащий по меньшей мере следующие
20 выбранные поля об анализе вредоносного программного обеспечения: ip-адреса, ключи реестра, мьютексы, user-агенты, маркеры, процессы и запускаемые программы, домен и тип запроса, файлы.

- В другом частном варианте реализации описываемого способа, результатом ансамбля классификаторов является итоговая оценка от -1 до 1, где -1 значит, что по
25 меньшей мере одна вредоносная программа совсем не принадлежит указанному семейству, а 1 - что по меньшей мере одна вредоносная программа принадлежит данному семейству.

В другом частном варианте реализации описываемого способа, по меньшей мере один ансамбль классификаторов способен выявлять отчеты, относящиеся к по меньшей мере одной группе вредоносных программ.

- 30 В другом частном варианте реализации описываемого способа, вектор признаков составляется на основе атрибутов, собранных с помощью регулярных выражений из поведенческого отчета.

- В другом частном варианте реализации описываемого способа, разделение происходит на основании базы данных размеченных известных файлов вредоносных
35 программ, по меньшей мере с помощью ssdeep, YARA, IDS, поведенческих сигнатур,

характерных поведенческих признаков, которые можно связать с конкретным семейством вредоносных программ.

Заявленный результат также достигается за счет системы поиска схожих вредоносных программ по результатам их динамического анализа включающая по меньшей мере:

- модуль фиксации, выполненный с возможностью фиксировать действия по меньшей мере одной вредоносной программы в, по меньшей мере, одном поведенческом отчете;
- вычислительное устройство, выполненное с возможностью осуществления вышеуказанного способа;
- модуль вывода.

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:

Фиг. 1, иллюстрирует систему поиска схожих вредоносных программ по результатам их динамического анализа.

Фиг. 2, иллюстрирует компьютерно-реализуемый способ поиска схожих вредоносных программ по результатам их динамического анализа.

Фиг. 3, иллюстрирует пример общей схемы компьютерного устройства.

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 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 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 поиска схожих вредоносных программ по результатам их динамического анализа, осуществляется посредством системы поиска схожих вредоносных программ по результатам их динамического анализа, представленной на Фиг.1, которая по меньшей мере содержит: модуль фиксации, выполненный с возможностью фиксировать действия по меньшей мере одной вредоносной программы в, по меньшей мере, одном поведенческом отчете (S10), вычислительное устройство, выполненное с возможностью осуществления способа поиска схожих вредоносных программ по результатам их динамического анализа (S20) и модуль вывода (S30).

10 Как представлено на Фиг. 2, заявленный компьютерно-реализуемый способ поиска схожих вредоносных программ по результатам их динамического анализа (100) реализован следующим образом.

На подготовительном этапе 101 выполняют динамический анализ известных вредоносных программ (этап 102). Для этого вредоносные программы запускают в изолированной среде («песочнице»).

На этапе 103, в процессе исполнения программ, посредством модуля фиксации (S10), фиксируются (например, записываются в логи) все выполняемые программами действия, например:

- a. процессы, запускаемые программой и параметры запуска каждого процесса;
- 20 b. файлы, создаваемые каждым процессом;
- c. мьютексы, создаваемые каждым процессом;
- d. ключи реестра, создаваемые каждым процессом;
- e. запись видео с экрана виртуальной машины во время работы вредоносной программы;
- 25 f. сетевая активность - всевозможная информация по взаимодействию вредоносной программы с сетью: тип запроса (GET, POST, PUT, HEAD), user agent, домен, ip-адрес, http/https, данные, передающиеся в теле запроса и так далее;
- g. маркеры вредоносности — что произошло в процессе выполнения вредоносной программы. Например, зафиксировано создание скрытых или системных файлов - первый маркер. Исполнение кода в неименованных регионах оперативной памяти - второй маркер. Обнаружены аномалии в структуре PE-файла - третий маркер. Создание копии самого себя - четвёртый маркер. Причем, некоторые маркеры могут помечаться красным, как подозрительные. Этап 103 заканчивается, когда накоплено достаточное количество сведений о поведении вредоносной программы, причем данные сведения представлены в виде поведенческих отчетов (отчетов JSON).

Отчет JSON состоит из множества полей, из которых выбирают следующие поля: ip-адреса, ключи реестра, мьютексы, user-агенты, маркеры, процессы и запускаемые программы, домен и тип запроса, файлы и создают по ним шесть классификаторов:

- по сети;
- 5 по маркерам;
- по ключам реестра;
- по процессам;
- по мьютексам;
- по файлам.

10 На этапе 104 разделяют накопленные поведенческие отчеты по группам таким образом, что отчеты, объединённые в одну группу, содержат похожие действия и принадлежат одному семейству вредоносных программ (или альтернативно одному коллективу разработчиков вредоносных программ).

Поведенческие отчеты разделяют на основании базы данных известных файлов вредоносных программ, которая размечена, например, с помощью следующих
15 инструментов: YARA правил, IDS сигнатур, поведенческих сигнатур, утилиты ssdeep.

YARA правила, представляют собой текстовые или бинарные образцы, в которых описываются формализованные признаки вредоносных программ (сигнатуры). Причем
каждое описание состоит из правил, которые представляют собой набор строк и некоторое
20 логическое выражение, на основе которого определяется логика срабатывания анализатора. В случае, если для исследуемого файла определяется хотя бы одно условие правила, то данный файл классифицируется как вредоносный файл. Такие правила пишутся экспертами и постоянно пополняются.

При запуске каждого файла в изолированной среде, он дополнительно проверяется
25 YARA-правилами.

IDS сигнатуры, представляют собой правила для выявления вредоносной активности по анализу сетевого трафика. В случае если анализируемый файл проявляет сетевую активность, по его трафику возможно дать более точную классификацию и понять какая именно вредоносная программа анализируется. Причем для обхода сигнатурного анализа
30 часто используется упаковка/шифрование исполняемого файла, однако анализ трафика не зависит от того какие модификации были сделаны с файлом, поэтому все его модификации точно идентифицируются.

Поведенческих сигнатуры, представляют собой правила, описывающие характерные признаки поведения для конкретного типа вредоносной программы. Это позволяет точно
35 классифицировать вредоносные программы, когда они не создают сетевой активности и не

обнаруживаются другими признаками. Такие правила пишутся экспертами и постоянно пополняются.

Утилита ssdeer, представляет собой инструмент для рекурсивного вычисления и сравнения контекстных частичных хэшей (нечёткое хеширование). При нечётком хешировании выявляются сходные файлы. Стоит отметить, что ssdeer разбивает файл на куски и запускает хэш-функцию для каждого из них. По результату этого хеширования строят окончательный хэш. Если изменяется только несколько байтов файла, то значение хэша данного файла незначительно изменится.

Имея базу размеченных файлов вредоносных программ, можно сравнивать хэши ssdeer и тем самым обнаруживать файлы с одинаковыми участками кода, которые еще не были размечены.

Поскольку файлы запускают в изолированной среде и фиксируют все выполняемые программами действия, то используя машинное обучение, возможно автоматически выявлять характерные поведенческие признаки для вредоносных программ. Имея базу размеченных файлов вредоносных программ, характерные поведенческие признаки можно связать с конкретным семейством вредоносных программ.

Например, выделенное ранее семейство, при запуске (выполнении) взаимодействует определенным образом с:

регистрами CPU и памятью (обращение к регистрам микропроцессора, ячейкам памяти, стекам, портам устройств);

ОС (вызовы WinAPI, NativeAPI, syscall);

изменениями в файловой системе (создание при запуске программы файлов (в т.ч. исполняемых), записей в реестре);

сетевых взаимодействия программы (как вредоносное программное обеспечение взаимодействует с управляющими центрами для передачи данных и приема команд);

перехваты и внедрения кода (внедрение или перехват inject кода или библиотек в другие процессы).

Сравнивая поведенческие признаки с признаками неклассифицированных вредоносных программ, можно выявлять модификации вредоносных программ. Так например, сравнивая с типичным поведением, характерным для вредоносного программного обеспечения, выявляют его аномалии при взаимодействии с системой и делают вывод о принадлежности вредоносной программы к определённому семейству, но с модификацией в поведении, которая может выражаться, например, в создании каких-либо дополнительных библиотек, или вызове дополнительных функций системы.

Количество вердиктов примерно равно количеству семейств вредоносных программ. То есть определяют, что конкретный файл вредоносной программы относится к семейству ISRStealer, а другой файл вредоносной программы к семейству Meterpreter.

Поведенческие отчеты об анализе вредоносных программ размечаются. Каждому поведенческому отчету присваивается одно или более семейств вредоносных программ. Одному поведенческому отчету может соответствовать множество семейств, например, в случае если одна вредоносная программа скачала и запустила другую вредоносную программу. Разметку можно проводить вручную или автоматически, за счет дополнительных специальных классификаторов.

Для создания ансамбля классификаторов обучают по меньшей мере один классификатор на по меньшей мере одном векторе, полученном по информации из по меньшей мере одного поля поведенческого отчета.

Для получения вектора признаков по одному полю поведенческого отчета, на этапе 105, при помощи регулярных выражений собирают атрибуты, которые записывают в вектор признаков, содержащий булевы значения. Полученный вектор подают на вход классификатора для обучения.

На этапе 106 обучают по меньшей мере один бинарный классификатор, на по меньшей мере одном векторе, полученном по информации из по меньшей мере одного поля поведенческого отчета. Например, первый бинарный классификатор обучается на векторе, созданном на основе поля маркеры, второй бинарный классификатор обучается на векторах, которые были получены по полям отчета «user-агенты», «ip адреса», «тип запроса» и «домен», и далее по такой схеме создаются оставшиеся бинарные классификаторы.

Над всеми бинарными классификаторами стоит взвешенная система, представляющая собой классификатор, которая считает вердикт от каждого бинарного классификатора и формирует на основе этого ответ о принадлежности данной вредоносной программы к определенному семейству.

Схема вынесения вердикта — это взвешенная система. В ней учитывается «ассигура» (точность на двух классах - данное семейство и все остальные) каждого классификатора. Причем «ассигура» берется исходя из работы классификатора на тестовых данных. Затем оно нормализуется, чтобы сумма всех «ассигур» от 6-ти классификаторов была равна 1.

Далее при классификации нового файла получившийся коэффициент домножается на нормализованную разницу «opt_proba» (оптимальная отсечка для данного классификатора, выше которой можно считать вредоносный файл принадлежащим

данному семейству) и «sig_proba» (результат вычисления вероятности отношения вредоносного файла к данному семейству по конкретному полю).

В результате просуммировав все произведения (их 6) получают оценку от -1 до 1, где -1 значит "файл точно не принадлежит данному семейству", а 1 - "файл точно принадлежит данному семейству".

Таким образом, на этапе 107 получается ансамбль бинарных классификаторов для нового семейства, который сможет в режиме детектирования выносить вердикт о принадлежности файла вредоносной программы к данному семейству.

Если после обработки файла всеми ансамблями семейств от каждого ансамбля получают ответ "нет" (то есть ни в одном случае не было превышено пороговое значение), то считается, что данный файл вредоносной программы относится к пока еще неизвестному семейству.

На рабочем этапе (110) запускают в изолированной среде вредоносную программу, принадлежность которой неизвестна (этап 111). На этапе 112 фиксируют, аналогично первому этапу, все выполняемые программой действия в поведенческий отчет. Затем проверяют отчет на принадлежность к одной из выделенных ранее групп отчетов. Это может быть выполнено, например, преобразованием отчета в вектор, и последующим запуском ранее обученного ансамбля классификаторов. На этапе 113 каждый из классификаторов формирует численную оценку вероятности, что анализируемая программа принадлежит к тому семейству известных вредоносных программ, на отчетах которых был ранее обучен данный ансамбль классификатор. Итоговую оценку выводят через модуль вывода (S30) на этапе 114.

Например, из отчетов извлекаются признаки, которые обнаружены в операционной системе в ходе ее работы. Эти признаки схожи с теми признаками, которые используются для определения факта вредоносности программы. Например, одним из признаков вредоносного поведения является факт добавления новой программы в список автоматически загружаемых при загрузке системы программ. Но если для анализа в «песочнице» важен сам факт, что программа была добавлена в список автозагрузки, то для поиска схожих вредоносных программ необходимо это действие соотнести с поведением конкретного семейства вредоносных программ. Поэтому для поиска схожих вредоносных программ важны следующие признаки: длина имени файла, расширение файла, какой из способов добавления в список автозагрузки используется. В общем используются следующие признаки:

- изменения в файловой системе;
- изменения в реестре операционной системы;

изменения в процессах, созданных в операционной системе;
сетевые взаимодействия;
вредоносные маркеры.

Извлеченные признаки отправляются на анализ ансамблю бинарных классификаторов, задача которого из общей массы признаков выявить, какие признаки характерны или, наоборот, не характерны для конкретного семейства, и на основе этих признаков вынести вердикт о принадлежности данной вредоносной программы определенному семейству вредоносного программного обеспечения.

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 JSON-отчётов, файлов с наборами данных, полученных с разных хостов, базы данных, содержащих записи зафиксированные в разные периоды для каждого пользователя 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, например, Ethernet карту, WLAN/Wi-Fi модуль, Bluetooth модуль, BLE модуль, NFC модуль, IrDa, RFID модуль, GSM модем и т.п. С помощью средств (305) 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.

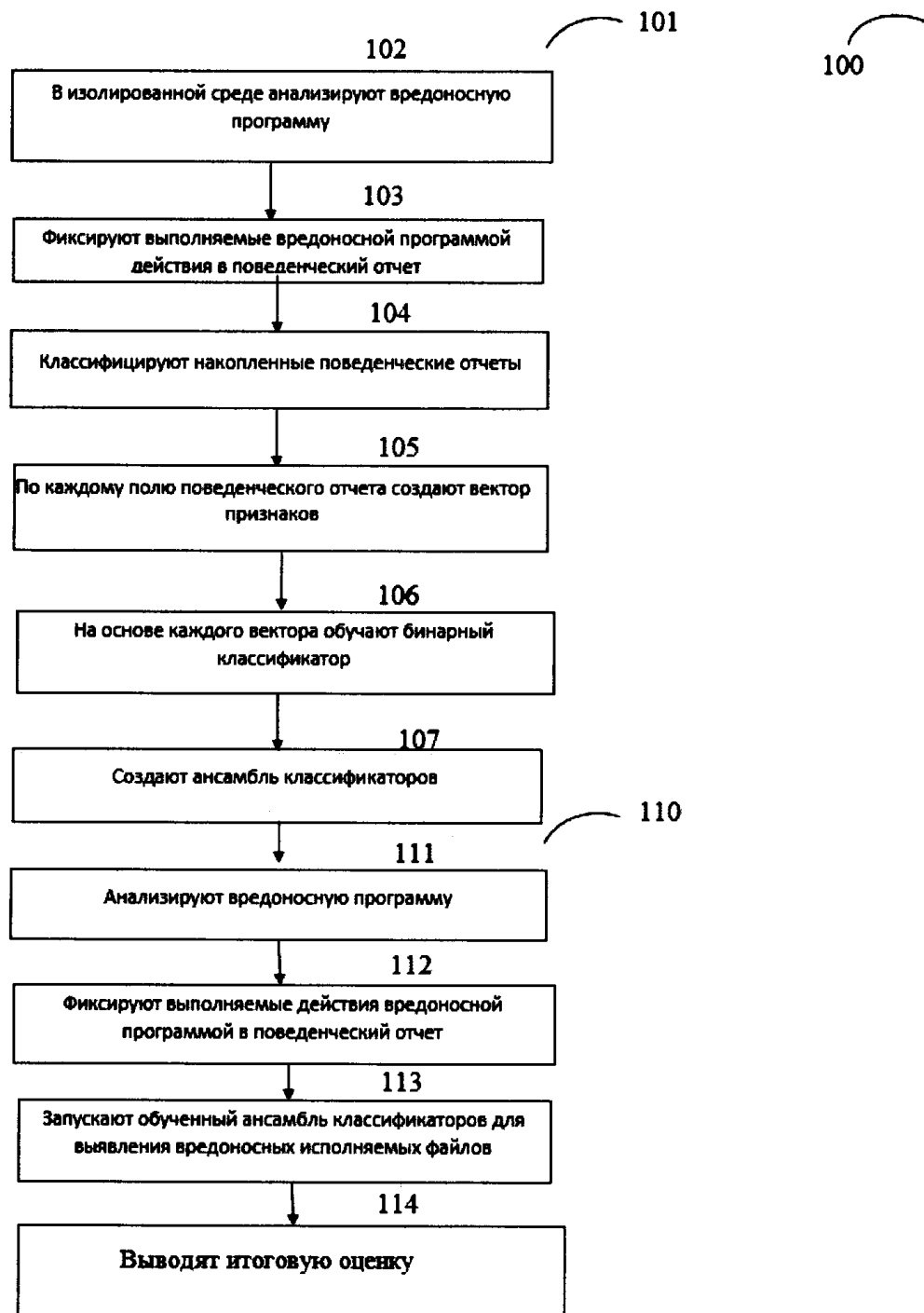
15

20

25

30

35



Фиг.2

- 102 Analyser dans un milieu isolé un programme malveillant
- 103 éterminer les actions exécutables par le programme malveillant dans un rapport de comportement
- 104 Classer les rapports de comportement accumulés
- 105 en fonction de chaque champ du rapport de comportement, créer un vecteur d'indices
- 106 Sur la base de chaque vecteur, réaliser l'apprentissage d'un classificateur binaire
- 107 générer un ensemble de classificateurs
- 111 Analyser le programme malveillant
- 112 déterminer les actions exécutables par le programme malveillant dans un rapport de comportement
- 113 initialiser l'ensemble des classificateurs binaires afin de révéler les fichiers malveillants exécutables
- 114 Générer une estimation finale

маркеры вредоносности.

3. Компьютерно-реализуемый способ по п.1, в котором отчет представляет собой отчет в формате JSON, содержащий по меньшей мере следующие поля об анализе вредоносного программного обеспечения: ip-адреса, ключи реестра, мьютексы, user-агенты, маркеры, процессы и запускаемые программы, домен и тип запроса, файлы.

4. Компьютерно-реализуемый способ по п.1, в котором результатом ансамбля классификаторов является итоговая оценка от -1 до 1, где -1 значит, что по меньшей мере одна вредоносная программа точно не принадлежит указанному семейству, а 1 - что по меньшей мере одна вредоносная программа точно принадлежит данному семейству.

5. Компьютерно-реализуемый способ по п.1, отличающийся тем, что по меньшей мере один ансамбль классификаторов способен выявлять отчеты, относящиеся к по меньшей мере одной группе вредоносных программ.

6. Компьютерно-реализуемый способ по п.1, в котором вектор признаков составляется на основе атрибутов, собранных с помощью регулярных выражений из поведенческого отчета.

7. Компьютерно-реализуемый способ по п.1, в котором разделение происходит на основании базы данных размеченных известных вредоносных файлов, по меньшей мере с помощью ssdeep, YARA, IDS, поведенческих сигнатур, характерных поведенческих признаков, которые можно связать с конкретным семейством вредоносных программ.

8. Система поиска схожих вредоносных программ по результатам их динамического анализа включающая по меньшей мере:

модуль фиксации, выполненный с возможностью фиксировать действия по меньшей мере одной вредоносной программы в, по меньшей мере, одном поведенческом отчете;

вычислительное устройство, выполненное с возможностью осуществления способа по пп. 1 -7;

модуль вывода.