

**СПОСОБ И СИСТЕМА ПРИНЯТИЯ РЕШЕНИЯ О НЕОБХОДИМОСТИ
АВТОМАТИЗИРОВАННОГО РЕАГИРОВАНИЯ НА ИНЦИДЕНТ**

ОБЛАСТЬ ТЕХНИКИ

- 5 Настоящее техническое решение относится к области вычислительной техники, в частности, к способу и системе принятия решения о необходимости автоматизированного реагирования на инцидент.

УРОВЕНЬ ТЕХНИКИ

- 10 Из источника информации RU 2610395 C1, 09.02.2017, известен способ, в котором загружают данные о системных событиях из всех компьютеров пользователей на сервер безопасности, регистрируют среди этих событий по меньшей мере одно системное событие, вызвавшее инцидент безопасности. Анализируют загруженные события путем поиска среди них таких, которые аналогичны событиям, предшествующим уже
- 15 зарегистрированному инциденту безопасности. Проводят корреляционный анализ данных о событиях, распределенных по времени и месту, с использованием дополнительных правил, включающих следующие действия: задают фоновые условия и уровень глубины анализа, формируют исходное множество правил для выполнения корреляционного анализа, производят отбор значимых правил в действующее множество, выявляют и
- 20 устраняют конфликты среди отобранных правил, проверяют для каждого правила из действующего множества соответствие фактической глубины анализа, проводят поиск и применяют решения для устранения последствий и предотвращения инцидента безопасности. Формируют отчет об инциденте безопасности.

- Из источника информации US 8,776,241 B2, 08.07.02014, известен способ
- 25 автоматического реагирования на инциденты, связанные с безопасностью в компьютерных сетях. Способ включает: управление клиентским компьютером по меньшей мере одним модулем набора защиты, который приспособлен для защиты информации, хранящейся на клиентском компьютере, и для обнаружения случаев инцидентов, связанных с безопасностью. Осуществляют регистрацию клиентским компьютером записей на уровне
- 30 событий, представляющих активность по меньшей мере одного модуля набора защиты. Обнаруживают, по меньшей мере, одним модулем набора защиты, инцидент, влияющий на информационную безопасность на клиентском компьютере, обнаружение выполняется на основе критериев обнаружения инцидента. В ответ на обнаружение инцидента, связывают клиентским компьютером выбранные из записей уровня, события с инцидентом, причем
- 35 ассоциирование выполняется на основе критериев ассоциирования инцидента.

- Предоставляют клиентским компьютером выбранные из записей уровня, удаленному серверу, события для анализа. Получают клиентским компьютером, по меньшей мере, одну рекомендацию о корректирующих действиях, которые должны автоматически выполняться на клиентском компьютере. Рекомендации о корректирующих действиях, принимаются с
- 5 удаленного сервера, в том числе инструкции по устранению инцидента. Осуществляют автоматическое выполнение клиентским компьютером инструкций по устранению инцидента. Получают клиентским компьютером инструкции по обновлению, по меньшей мере, одного из: критериев обнаружения инцидентов, критериев ассоциирования инцидентов или их комбинации, с новым набором соответствующих критериев.
- 10 В известных из уровня техники источниках обнаружение инцидента происходит в самой системе реагирования. В предлагаемом решении, сигнал о найденном инциденте передают в систему автоматизированного реагирования вместе со свойствами угрозами, посредством сторонних систем поиска угроз. Кроме того, в предлагаемом решении, определяется, предотвращена найденная угроза или нет, и в случае определения, что угроза
- 15 не предотвращена, выбирают одну из заранее определенных категорий реагирования, где для каждой категории есть свои инструкции по реагированию.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

- Технической проблемой, на решение которой направлено заявленное техническое
- 20 решение, является создание компьютерно-реализуемого способа и системы принятия решения о необходимости автоматизированного реагирования на инцидент, которые охарактеризованы в независимых пунктах формулы. Дополнительные варианты реализации настоящего изобретения представлены в зависимых пунктах изобретения.

- Технический результат заключается в осуществлении автоматизированного
- 25 реагирования на инцидент.

Заявленный результат достигается за счет осуществления компьютерно-реализуемого способ принятия решения о необходимости автоматизированного реагирования на инцидент, содержащий этапы, на которых:

- при получении от сторонних систем, посредством интерфейсного модуля, сигнала
- 30 по меньшей мере об одном инциденте, информацию об инциденте передают в аналитический модуль, где:

определяют, был ли инцидент предотвращён ранее, и если нет, то

определяют уровень опасности инцидента, и если уровень опасности превышает заранее заданный порог,

осуществляют, посредством аналитического модуля и модуля реагирования, реагирование на инцидент.

В частном варианте реализации описываемого способа, сведения об инциденте содержат, по меньшей мере, категорию инцидента, уровень угрозы инцидента, имя хоста, на котором произошёл инцидент и степень уверенности в том, что инцидент не является ложным срабатыванием.

В другом частном варианте реализации описываемого способа, дополнительно относят категорию инцидента к одной из трёх категорий реагирования.

В другом частном варианте реализации описываемого способа, если инцидент относится к первой категории реагирования, то посредством модуля реагирования останавливают вредоносный процесс и изолируют хост.

В другом частном варианте реализации описываемого способа, если инцидент относится ко второй категории реагирования, то посредством аналитического модуля определяют с какой учетной записи происходит активность, и если учетная запись не относится к привилегированным учетным записям, то ее блокируют.

В другом частном варианте реализации описываемого способа, если активность происходит с привилегированной учетной записи, то степень уверенности сравнивают с заранее заданным порогом, и если степень уверенности меньше заранее заданного порога, то привилегированную учетную запись блокируют.

В другом частном варианте реализации описываемого способа, блокируют привилегированную запись, если количество заблокированных привилегированных учетных записей за заранее заданное время менее N_1 записей.

В другом частном варианте реализации описываемого способа, если инцидент относится к третьей категории реагирования, то определяют, посредством аналитического модуля, каким процессом порождён инцидент, и является ли серверной операционная система хоста, на котором произошёл инцидент.

В другом частном варианте реализации описываемого способа, если инцидент порожден системным процессом, и операционная система хоста серверная, то посредством модуля реагирования снимают содержимое оперативной памяти.

В другом частном варианте реализации описываемого способа, снимают содержимое оперативной памяти, если за заранее заданное время было совершено менее N_2 реагирований.

В другом частном варианте реализации описываемого способа, если инцидент порожден не системным процессом, а операционная система хоста серверная то

посредством модуля реагирования снимают содержимое оперативной памяти и останавливают процесс.

В другом частном варианте реализации описываемого способа, снимают содержимое оперативной памяти и останавливают процесс, если за заранее заданное время
5 было совершено менее N_3 реагирований.

В другом частном варианте реализации описываемого способа, если операционная система хоста не серверная, то посредством модуля реагирования изолируют от сети хост, на котором обнаружен инцидент.

В другом частном варианте реализации описываемого способа, изолируют хост от
10 сети, если за заранее заданное время было изолированного менее N_4 хостов.

В другом частном варианте реализации описываемого способа, процесс автоматического реагирования, посредством модуля реагирования, осуществляют на уровне файла, хоста и корпоративной сети.

В другом частном варианте реализации описываемого способа, реагирование на
15 уровне файла включает в себя, полностью или частично, следующие шаги:

блокируют по меньшей мере один вредоносный файл и отправляют его в карантин;

отправляют по меньшей мере один вредоносный файл на динамический анализ в изолированную среду;

ищут по меньшей мере один вредоносный файл, являющийся дочерним, на по
20 меньшей мере одном хосте, и удаляют его;

завершают вредоносный процесс.

В другом частном варианте реализации описываемого способа, реагирование на уровне хоста включает в себя, полностью или частично, следующие шаги:

собирают сведения об инциденте;

25 создают копию содержимого оперативной памяти;

создают посекторную копию энергонезависимого запоминающего устройства;

изолируют хост от сети;

блокируют запуск любых приложений, кроме оригинальных программ, разработанных производителем операционной системы.

30 В другом частном варианте реализации описываемого способа, информация об инциденте включают в себя, по меньшей мере, сведения о программах, автоматически загружаемых при загрузке операционной системы, Prefetch-файлы, запущенные процессы, системные журналы событий, содержимое временных директорий.

В другом частном варианте реализации описываемого способа, реагирование на
35 уровне корпоративной сети включает в себя, полностью или частично, следующие шаги:

блокируют учетную запись пользователя на уровне домена;
запускают файлы сценария по работе с инцидентами;
отправляют отчет.

Заявленный результат также достигается за счет системы для принятия решения о
5 необходимости автоматизированного реагирования на инцидент, состоящая из следующих функциональных модулей:

интерфейсный модуль, выполненный с возможностью получения от внешних систем сигналов об обнаружении инцидента;

аналитический модуль, выполненный с возможностью определять условия и
10 выбирать правила автоматизированного реагирования;

модуль реагирования, выполненный с возможностью выполнения автоматизированного реагирования при выполнении вышеуказанного способа.

ОПИСАНИЕ ЧЕРТЕЖЕЙ

15 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 принятия решения о необходимости
20 автоматизированного реагирования на инцидент.

Фиг.2, иллюстрирует компьютерно-реализуемый способ принятия решения о необходимости автоматизированного реагирования на инцидент.

Фиг. 3, иллюстрирует один из возможных алгоритмов компьютерно-реализуемого способа принятия решения о необходимости автоматизированного реагирования на
25 инцидент.

Фиг. 4, иллюстрирует пример общей схемы вычислительного устройства.

ДЕТАЛЬНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

В приведенном ниже подробном описании реализации изобретения приведены
30 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
35 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.

- 5 Заявленный компьютерно-реализуемый способ предназначен для реализации в виде обособленного алгоритма в работе большой многокомпонентной системы. Многокомпонентная система может быть выполнена по-разному и содержать разные функциональные блоки или подсистемы, в том числе, например, антивирусную программу, изолированную среду («песочницу»), платформу детонации вредоносного программного обеспечения, иметь подключение к центру быстрого реагирования (CERT), и так далее. Эти
10 и другие функциональные блоки или подсистемы, не входящие в состав описываемой системы автоматизированного реагирования на инцидент, далее в тексте данной заявки будут называться «внешними системами». При этом подразумевается, что они действуют согласованно с описываемой системой, но сами по себе не входят в её состав.
- 15 Компьютерно-реализуемый способ принятия решения о необходимости автоматизированного реагирования на инцидент, осуществляется посредством системы принятия решения о необходимости автоматизированного реагирования на инцидент, представленной на Фиг.1, которая состоит из следующих функциональных модулей: интерфейсный модуль, выполненный с возможностью получения от внешних систем
20 сигналов об обнаружении инцидента (S10), аналитический модуль, выполненный с возможностью определять условия и выбирать способы автоматизированного реагирования (S20), а также с возможностью доступа к базе данных (S25) с обеспечением получения из неё данных и сохранения в неё данных, и модуль реагирования (S30), выполненный с возможностью выполнения автоматизированного реагирования при
25 выполнении вышеуказанного способа.

Как представлено на Фиг.2, заявленный компьютерно-реализуемый способ принятия решения о необходимости автоматизированного реагирования на инцидент (100) реализован следующим образом.

- 30 Автоматизированное реагирование реализуется в случае обнаружения угрозы или иного инцидента компьютерной безопасности. При этом подразумевается, что собственно поиск и обнаружение угрозы или инцидента выполняется внешними системами. При обнаружении угрозы на описываемую систему подается соответствующий сигнал, после чего данной системой выполняется автоматизированное реагирование.

На этапе 110, как показано на Фиг.2, посредством интерфейсного модуля (S10 на Фиг.1) получают сигнал по меньшей мере об одном инциденте. Сигнал об инциденте характеризуется по меньшей мере одним из следующих свойств.

Категория угрозы (Category). Категория указывает, какой именно инцидент обнаружен: работа вредоносной программы определённого вида, например, «шифровальщика», «червя», «трояна», вредоносная активность, связанная с перемещением по сети, признаки развития целенаправленной хакерской атаки (так называемой АРТ), и так далее.

Уровень угрозы (Severity). Уровень обычно зависит от категории угрозы. Например, при обнаружении работы нежелательной программы, такой как рекламная программа, adware, уровень угрозы может быть низким. В то же время, при обнаружении работы программы-шифровальщика или «червя» уровень угрозы может быть высоким. Оценка уровня угрозы формируется той системой, которая обнаружила угрозу, например, платформой детонации вредоносного программного обеспечения, известной как TDS Polygon, или изолированной средой - «песочницей». Оценка может быть бинарной (0 или 1), либо категорийной, когда любая угроза относится к одной из четырёх, например, наперёд заданных категорий, таких, например, как критическая, высокая, средняя, низкая.

Степень уверенности (Reliability). Это численный показатель, соответствующий уверенности внешней системы, обнаружившей угрозу, в том, что вердикт об обнаружении угрозы не является ложным срабатыванием.

Имя или адрес хоста, на котором произошел инцидент. В материалах настоящей заявки, под хостом понимается узел сети. 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, например, так называемые виртуальные хосты Apache и т.д.

Также сигнал об инциденте может содержать дополнительные сведения, например, имя и контрольную сумму файла вредоносной программы, срабатывание которой обнаружено, IP-адрес или доменное имя внешнего по отношению к защищаемой сети веб-сервера, к которому отправлен запрос с одного из хостов защищаемой сети, название учетной записи, со стороны которой наблюдается перемещение по защищаемой сети и т.д.

Далее поступившие сведения об инциденте передают в аналитический модуль (S20 на Фиг.1). На этапе 120, как показано на Фиг. 2, посредством аналитического модуля (S20 на Фиг. 1) определяют, был ли предотвращен данный инцидент ранее, или нет (шаг 121 на

Фиг. 3). Данный шаг направлен на исключение реагирования в тех случаях, когда инцидент заведомо не несёт угрозы. Например, когда срабатывание вредоносной программы произошло в «песочнице», в изолированной среде, или повторно обнаружен уже заблокированный ранее вредоносный файл. В таких случаях автоматизированное реагирование на инцидент не проводится.

Определение, несёт ли данный инцидент угрозу, выполняется аналитическим модулем (S20 на Фиг. 1) путём проверки по базе данных (S25 на Фиг. 1). Данная база содержит сведения обо всех хостах, входящих в состав сети, в которой работает описываемая система, а также обо всех процедурах реагирования, выполненных системой за заранее заданный период времени, например, за последние сутки.

Если имя или адрес хоста, на котором произошел инцидент, совпадает с одним из имен или адресов хостов, на которых расположены «песочницы», системы детонации вредоносных программ и т.п. изолированные среды, то считается, что инцидент предотвращён и реагирование на инцидент не производится.

Если имя или контрольная сумма файла вредоносной программы, срабатывание которой обнаружено, совпадает с одним из имён или контрольных сумм файлов вредоносных программ, уже заблокированных системой на данном хосте в ходе одной из процедур реагирования, выполненных за заданный период времени, то считается, что инцидент предотвращен и реагирование не производится.

В тех случаях, когда сигнал об инциденте не содержит имени или контрольной суммы файла вредоносной программы, например, если инцидент представляет собой перемещение по сети, запрос к внешнему IP-адресу (входящему в список вредоносных адресов) или признаки развития АРТ, считается, что инцидент не предотвращён, и реагирование необходимо.

Такое же решение принимается в тех случаях, когда инцидент происходит на хосте, не являющемся «песочницей» или когда ранее проведённое реагирование на данный вредоносный файл не зафиксировано.

Если определяется, что инцидент не предотвращен, то определяется уровень опасности инцидента (этап 130 на Фиг. 2). Если уровень опасности инцидента меньше, чем заранее заданное значение, то реагирование не выполняется. В случае, если значение уровня опасности инцидента больше, чем заранее заданное значение, выполняется автоматизированное реагирование (этап 140 на Фиг. 2). В зависимости от поступивших сведений об инциденте, автоматизированное реагирование может выполняться различным образом. Неограничивающий пример дальнейших возможных шагов алгоритма автоматизированного реагирования показан на Фиг.3.

При этом следует понимать, что алгоритм, показанный на Фиг.3, является именно примером, и возможны многочисленные варианты альтернативных способов реализации описанной системы.

В частности, количество перечисленных категорий реагирования (ветвей алгоритма на Фиг.3) может быть более или менее трёх. Например, в отличие от Фиг.3, инцидент вида «распространение трояна» и инцидент вида «АРТ» могут принадлежать к двум различным категориям реагирования. Аналогично, инциденты вида «распространение червя», «запуск программы уничтожения данных» и «запуск шифровальщика» могут принадлежать к трём различным категориям реагирования, и т.д.

Альтернативно, группировка инцидентов различных видов по категориям реагирования также может отличаться от показанной на Фиг.3. Например, в одном из возможных вариантов реализации описанной системы, инцидент вида «распространение трояна» (шаг 153 на Фиг.3) и инцидент вида «распространение червя» (шаг 151 на Фиг.3) могут быть помещены в одну категорию реагирования, а не в разные, как в нижеописанном случае.

Реагирование выполняется на следующих уровнях:

на уровне файла;

на уровне хоста;

на уровне корпоративной сети.

Реагирование на уровне файла включает:

- блокировку вредоносного файла и отправку его в карантин;
- отправку вредоносного файла на динамический анализ в изолированную среду (в «песочницу» любого известного вида или в платформу детонации вредоносного программного обеспечения любого известного вида, например, в TDS Polygon).

- осуществление поиска оригинальных и дочерних вредоносных файлов на всех хостах и осуществление их удаления;

- остановку вредоносного процесса.

Реагирование на уровне хоста включает:

- сбор информации об инциденте, которая необходима для оперативного исследования. Информация об инциденте, содержит, по меньшей мере, сведения о программах в автозагрузке, Prefetch-файлах, запущенных процессах, системные журналы событий, содержимое временных директорий;

- снятие содержимого оперативной памяти;

- создание посекторной копии энергозависимого запоминающего устройства (например, HDD, SDD и т.д.);

- изолирование хоста от сети;

- блокировку запуска любых приложений, кроме оригинальных программ, разработанных производителем операционной системы.

Реагирование на уровне корпоративной сети включает:

- блокировку учетной записи пользователя на уровне домена;

- запуск файлов сценария по работе с инцидентами. Например, добавление в черный список серверов рассылки вредоносных писем или блокировка IP-адресов серверов управления вредоносным программным обеспечением на уровне межсетевых экранов.

Реагирование на разных уровнях осуществляется в зависимости от инцидента, который произошел, его свойств, а также целесообразности выполнения конкретных мер. Так, реагирование на разных уровнях включает выполнение вышеописанных шагов полностью или частично.

Далее в ходе этапа 130 (на Фиг. 2) переходит к определению категории инцидента (шаг 150 на Фиг. 3). В рамках неограничивающего примера возможной реализации заявленного изобретения может быть определено, по меньшей мере три категории реагирования, как показано на Фиг. 3.

К первой категории реагирования (151) в рамках данного примера, относят инциденты, порожденные угрозами следующих видов, но не ограничиваясь: «шифровальщик», «червь», программа для уничтожения данных.

Ко второй категории реагирования (152) в рамках данного примера, относят инциденты, связанные с перемещением учетной записи по сети.

К третьей категории (153) реагирования в рамках данного примера, относят все остальные инциденты, не относящиеся к первой или второй категории реагирования, например, «троян», «АРТ» и так далее.

Если инцидент в рамках данного примера относится к первой категории реагирования (151), то посредством модуля реагирования (S30 на Фиг. 1), на этапе 140 в соответствии с Фиг. 2, на уровне файла останавливают вредоносный процесс (шаг 141 на Фиг. 3), затем на уровне хоста изолируют хост (шаг 142 на Фиг. 3).

Пример реализации.

Один из сотрудников организации, компьютерная сеть которой находится под защитой системы кибербезопасности, включающей в себя систему, реализующую данный способ, получает с адреса администратора домена, чья учётная запись была скомпрометирована, e-mail с вложением и текстом, содержащим просьбу срочно

ознакомиться с вложенным документом. Сотрудник открывает вложенный документ, в результате чего происходит заражение его компьютера вредоносной программой типа «червь». Последний начинает распространяться в локальной сети.

На по меньшей мере одной из «внешних» систем постоянно осуществляется поиск
5 угроз. При обнаружении распространения «червя» «внешняя» система сформирует и передаст системе, реализующей описываемый способ, сигнал об инциденте, который поступит на интерфейсный модуль системы (S10 на Фиг.1), реализующей описываемый способ.

Данный сигнал будет иметь следующие свойства:

10 Уровень угрозы (Severity): критический;

Категория угрозы (Category): «червь»;

Степень уверенности (Reliability): 99%;

Сегмент сети, где находится компьютер, на котором произошел инцидент: название сегмента;

15 Рабочая группа \ домен, к которой он принадлежит: имя домена \ рабочей группы;

Чьим (по должности) рабочим местом является этот компьютер: компьютер сотрудника.

Таких сигналов в системе может быть больше, поскольку какие-то ещё компьютеры в локальной сети тоже могут оказаться заражёнными «червём» до срабатывания системы
20 реагирования на инцидент. Действия описываемой системы по каждому из таких сигналов будут идентичны.

В соответствии с Фиг.3, шаг 121, аналитический модуль (S20 на Фиг.1) определит, что срабатывание вредоносной программы произошло не в «песочнице» и что данный вредоносный файл ранее заблокирован не был. Поэтому система в соответствии с Фиг. 3,
25 на шаге 130 оценит уровень угрозы и поскольку он превышает установленный в данном примере низкий уровень, на шаге 150 проведёт автоматизированное реагирование на инцидент.

Поскольку категория угрозы «червь», в описываемом примере дальнейшее реагирование будет производиться по первой категории реагирования (шаг 151 на Фиг.3).

30 На уровне файла на шаге 141 (Фиг.3) будут выполнены следующие шаги:

блокировка вредоносного файла и отправка его в карантин;

дополнительно может быть выполнена также отправка вредоносного файла на динамический анализ (зависит от того, известна ли данная разновидность «червя»);

поиск оригинального и дочерних файлов на всех компьютерах и их удаление;

35 завершение вредоносного процесса.

На уровне хоста на шаге 142 (Фиг.3) могут быть выполнены следующие шаги:
изоляция хоста от сети (чтобы остановить распространение «червя»);

сбор необходимых доказательств. Архив, включающий в себя информацию, необходимую для оперативного исследования (данные о программах в автозагрузке, Prefetch-файлах, запущенных процессах, системные журналы событий, содержимое временных директорий и т.п) может быть создан на данном шаге для изучения способа проникновения вредоносной программы;

Если «червь» не несёт какой-либо дополнительной нагрузки, то есть других вредоносных программ, распространяющихся вместе с ним (предположим, не несёт), то снятие содержимого оперативной памяти и создание посекторной копии энергозависимого запоминающего устройства могут не выполняться.

На уровне корпоративной сети будет выполнена отправка отчётности о результатах реагирования ответственным лицам. На этом автоматизированное реагирование на описанный инцидент завершится (конец примера реализации).

Если окажется, что инцидент относится ко второй категории реагирования (шаг 152 на Фиг.3), то определяется, посредством аналитического модуля (S20 на Фиг.1), с какой учетной записи происходит активность, и если учетная запись не относится к привилегированным учетным записям, что определяется на шаге 148 (Фиг.3), и количество заблокированных учетных записей за заранее заданное время менее N_1 записей, где N_1 некоторое заранее заданное целое число, то ее блокируют (шаг 143 на Фиг.3) на уровне корпоративной сети посредством модуля реагирования (S30 на Фиг.1), что соответствует этапу 140 на Фиг.2. В том случае, если количество заблокированных привилегированных учетных записей за заранее заданное время более N_1 записей, то реагирование на инцидент не выполняют.

В материалах настоящей заявки, под привилегированной учетной записью понимается учетная запись, которая имеет право устанавливать, изменять и управлять какой-либо информационной системой или устройством. В корпоративной ИТ-инфраструктуре иметь привилегированную учетную запись могут, например, системные администраторы, администраторы приложений, баз данных, облачных сервисов, веб-сайтов, а также руководители некоторых отделов, например, отдела безопасности, отдела кибербезопасности и т.д.

В том случае, если активность происходит с привилегированной учетной записи, то степень уверенности (Reliability) угрозы на шаге 148 (Фиг.3) сравнивают с заранее заданным порогом (например, значение порога $R=80\%$) и если степень уверенности меньше, чем заранее заданный порог, а также если количество заблокированных

привилегированных учетных записей за заранее заданное время менее N_1 записей, то посредством модуля реагирования (S30 на Фиг.1), в соответствии с этапом 140 на Фиг.2, на уровне корпоративной сети, привилегированную учетную запись блокируют (шаг 143 на Фиг.3) на уровне корпоративной сети. В том случае, если количество заблокированных привилегированных учетных записей за заранее заданное время более N_1 записей, то реагирование на инцидент не выполняют.

Если инцидент относится, в рамках неограничивающего примера, к третьей категории реагирования (шаг 153 на Фиг.3), то определяют, посредством аналитического модуля (S20 на Фиг.1), каким процессом порождён инцидент (шаг 122 на Фиг.3), и является ли серверной операционная система хоста, на котором произошёл инцидент (шаг 123 на Фиг.3).

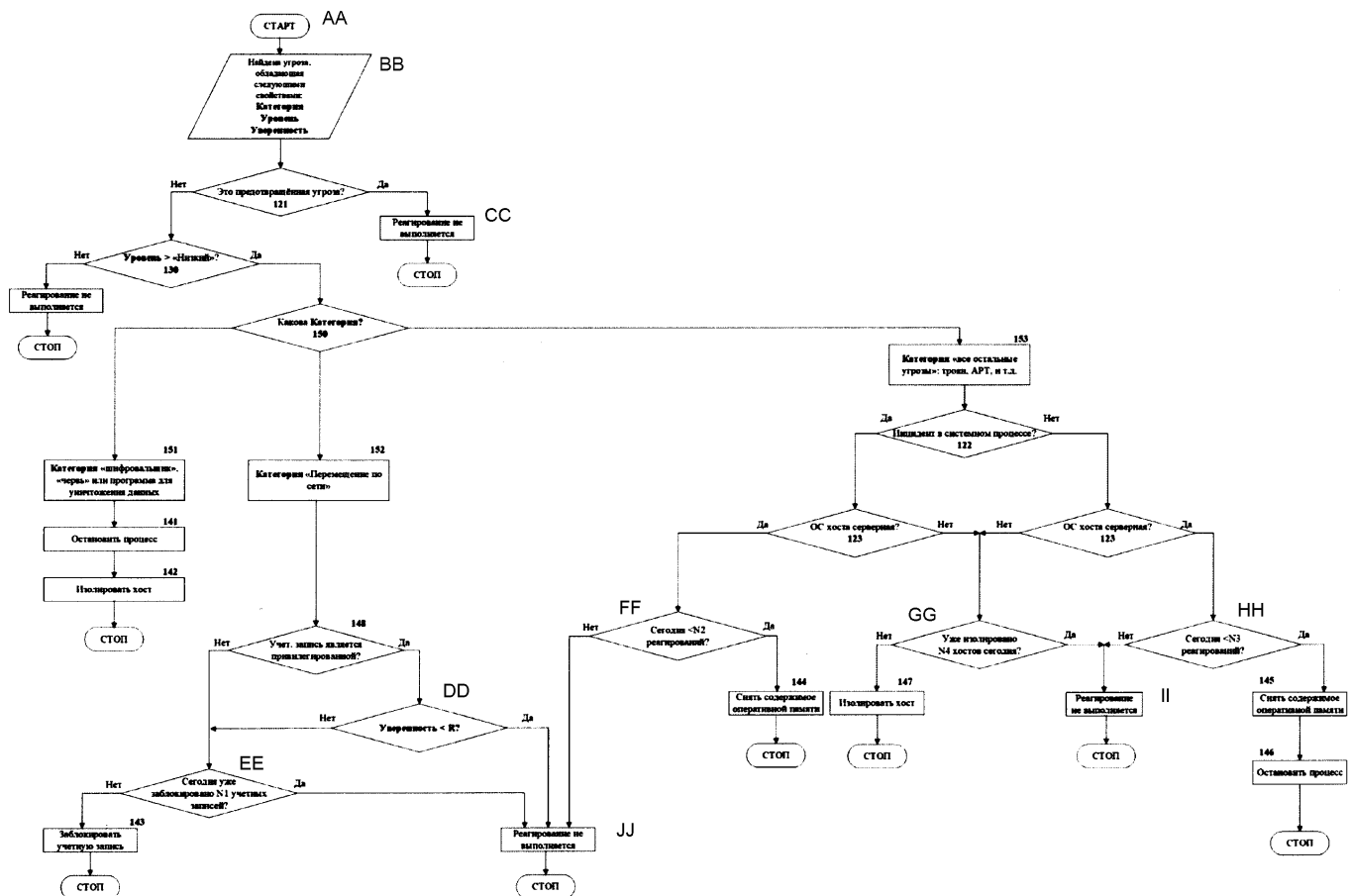
В том случае, если инцидент порожден системным процессом, и операционная система хоста серверная, то посредством модуля реагирования (S30 на Фиг.1), в соответствии с этапом 140 на Фиг.2, в порядке реагирования на уровне хоста снимают содержимое оперативной памяти (шаг 144 на Фиг.3). Содержимое оперативной памяти снимают, если за заранее заданное время было совершено менее N_2 реагирований, где N_2 некоторое заранее заданное целое число. Если за заранее заданное время было совершено более N_2 реагирований, то реагирование на инцидент не выполняют.

В том случае, если инцидент порожден не системным процессом, а операционная система хоста серверная, то посредством модуля реагирования (S30 на Фиг.1), в соответствии с этапом 140 на Фиг.2, в порядке реагирования на уровне хоста снимают содержимое оперативной памяти (шаг 145 на Фиг.3) и останавливают вредоносный процесс (шаг 146 на Фиг.3). Содержимое оперативной памяти снимают и останавливают процесс, если за заранее заданное время было совершено менее N_3 реагирований, где N_3 некоторое заранее заданное целое число. Если за заранее заданное время не было совершено менее N_3 реагирований, то реагирование на инцидент не выполняют.

В том случае, если операционная система хоста, на котором произошел инцидент, не серверная, то посредством модуля реагирования (S30 на Фиг.1), в соответствии с этапом 140 на Фиг.2, в порядке реагирования на уровне хоста изолируют от сети хост (шаг 147 на Фиг.3), на котором обнаружен инцидент. Хост изолируют от сети в том случае, если за заранее заданное время было изолированного менее N_4 хостов, где N_4 некоторое заранее заданное целое число, в ином случае реагирование на инцидент не выполняют.

Пример реализации.

Злоумышленник получил удалённый доступ к операционной системе одного из хостов контролируемой сети под привилегированной учётной записью, например, под



Фиг.3

AA DÉBUT

BB STOP

CC Détection de menace avec les propriétés suivantes: catégorie, gravité, fiabilité

DD Aucune réponse mise en œuvre

EE Aucune réponse mise en œuvre

FF Fiabilité < R ?

GG Compte N1 déjà bloqué aujourd'hui ?

HH Non

II Oui

JJ Hôte N4 déjà isolé aujourd'hui ?

KK < N3 réponses aujourd'hui ?

LL Aucune réponse mise en œuvre

MM < N2 réponses aujourd'hui ?

NN Aucune réponse mise en œuvre

121 menace préalablement empêchée ?

122 Incident dans le processus système ?

123 OS Hôte = OS Serveur ?

130 Gravité « basse » ?

141 Arrêter le processus

142 Isoler l'hôte

143 Bloquer le compte

144 Réduire le contenu RAM

145 Réduire le contenu RAM

146 Arrêter le processus

147 Isoler l'hôte

148 Compte = compte privilégié ?

150 Quelle catégorie ?

151 Catégorie « cryptage », « ver » ou programme de destruction de données

152 Catégorie mouvement dans le réseau

153 Catégorie « toutes les autres menaces », Cheval de Troie, APT, etc.

Поскольку категория угрозы в данном случае будет иметь значение «АРТ», то реагирование в данном примере будет производиться по ветви алгоритма, соответствующей шагу 153 на Фиг.3, к которому в рассматриваемом примере относится АРТ. Поскольку инцидент произошёл не в системном процессе (процессы интерпретатора cmd.exe к системным не относятся), а операционная система хоста, на котором произошёл инцидент, не является серверной, дополнительно проверяется, изолировали ли сегодня (в день обнаружения угрозы) N_4 хостов; допустим, $N_4=5$. Системой в текущий день ещё не было изолировано 5 хостов, поэтому реагирование будет проведено по типу «изолировать хост» (шаг 147 на Фиг.3).

Поскольку вредоносные файлы в данном инциденте не задействованы, реагирование на уровне файла не производится.

На уровне хоста может быть проведён сбор необходимых доказательств, составлен и отправлен на управляющий («внешний») сервер архив, включающий в себя информацию необходимые для оперативного исследования. В данном случае это может быть информация обо всех запущенных в настоящий момент процессах, о присутствующих в автозагрузке ярлыках, Prefetch-файлах, системные журналы событий, содержимое временных директорий и т.п. После получения архива будет выполнена изоляция хоста от сети, вследствие этого злоумышленник, получивший контроль над системой, утратит возможность продолжать разведывательные действия, поскольку удалённое соединение при этом будет прервано, без возможности восстановления.

Поскольку вредоносные файлы в данном инциденте не задействованы, снятие содержимого оперативной памяти и посекторной копии энергозависимого запоминающего устройства может не выполняться.

На уровне корпоративной сети будет выполнена блокировка учетной записи пользователя, чьи учетные данные скомпрометированы, на уровне домена. Кроме того, отчётность о результатах реагирования будет отправлена ответственным лицам. На этом автоматизированное реагирование на инцидент завершится (конец примера реализации).

На Фиг. 4 далее будет представлена общая схема вычислительного устройства (400), обеспечивающего обработку данных, необходимую для реализации заявленного решения.

В общем случае устройство (400) содержит такие компоненты, как: один или более процессоров (401), по меньшей мере одну память (402), средство хранения данных (403), интерфейсы ввода/вывода (404), средство В/В (405), средства сетевого взаимодействия (406).

Процессор (401) устройства выполняет основные вычислительные операции, необходимые для функционирования устройства (400) или функциональности одного или

более его компонентов. Процессор (401) исполняет необходимые машиночитаемые команды, содержащиеся в оперативной памяти (402).

Память (402), как правило, выполнена в виде ОЗУ и содержит необходимую программную логику, обеспечивающую требуемый функционал.

- 5 Средство хранения данных (403) 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 (403) позволяет выполнять долгосрочное хранение различного вида информации, например, вышеупомянутых файлов с наборами данных, полученных с разных хостов базы данных, содержащих записи зафиксированные
10 в разные периоды для каждого пользователя временных интервалов, идентификаторов пользователей и т.п.

Интерфейсы (404) 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.

- 15 Выбор интерфейсов (404) зависит от конкретного исполнения устройства (400), которое может представлять собой персональный компьютер, мейнфрейм, серверный кластер, тонкий клиент, смартфон, ноутбук и т.п.

- В качестве средств В/В данных (405) могут использоваться: клавиатура джойстик, дисплей (сенсорный дисплей), проектор, тачпад, манипулятор мышь, трекбол, световое
20 перо, динамики, микрофон и т.п.

- Средства сетевого взаимодействия (406) 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 (406) обеспечивается организация
25 обмена данными по проводному или беспроводному каналу передачи данных, например, WAN, PAN, LBC (LAN), Интранет, Интернет, WLAN, WMAN или GSM.

- Компоненты устройства (400) сопряжены посредством общей шины передачи данных (410). В настоящих материалах заявки было представлено предпочтительное раскрытие осуществление заявленного технического решения, которое не должно
30 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.

Формула

1. Компьютерно-реализованный способ принятия решения о необходимости автоматизированного реагирования на инцидент, содержащий этапы, на которых:
- при получении от сторонних систем, посредством интерфейсного модуля, сигнала
- 5 по меньшей мере об одном инциденте, сведения об инциденте передают в аналитический модуль, где:
- определяют, был ли инцидент предотвращён ранее, и если нет, то
- определяют уровень опасности инцидента, и если уровень опасности превышает заранее заданный порог,
- 10 осуществляют, посредством аналитического модуля и модуля реагирования, реагирование на инцидент.
2. Способ по п.1, отличающийся тем, что сведения об инциденте содержат, по меньшей мере, категорию инцидента, уровень угрозы инцидента, имя или адрес хоста, на котором произошёл инцидент и степень уверенности в том, что инцидент не является
- 15 ложным срабатыванием.
3. Способ по п.2, отличающийся тем, что дополнительно относят категорию инцидента к одной из нескольких заранее определенных категорий реагирования.
4. Способ по п. 3, отличающийся тем, что если инцидент относится к первой категории реагирования, то посредством модуля реагирования останавливают вредоносный
- 20 процесс и изолируют хост.
5. Способ по п.3, отличающийся тем, что если инцидент относится ко второй категории реагирования, то посредством аналитического модуля определяют с какой учетной записи происходит активность, и если учетная запись не относится к привилегированным учетным записям, то ее блокируют.
- 25 6. Способ по п.5, отличающийся тем, что если активность происходит с привилегированной учетной записи, то степень уверенности сравнивают с заранее заданным порогом, и если степень уверенности меньше заранее заданного порога, то привилегированную учетную запись блокируют.
7. Способ по п.6, отличающийся тем, что блокируют привилегированную
- 30 запись, если количество заблокированных привилегированных учетных записей за заранее заданное время менее N_1 записей.
8. Способ по п.3, отличающийся тем, что если инцидент относится к третьей категории реагирования, то определяют, посредством аналитического модуля, каким процессом порождён инцидент, и является ли серверной операционная система хоста, на
- 35 котором произошёл инцидент.

9. Способ по п.8, отличающийся тем, что если инцидент порожден системным процессом, и операционная система хоста серверная, то посредством модуля реагирования снимают содержимое оперативной памяти.
10. Способ по п. 9 отличающийся тем, что снимают содержимое оперативной
5 памяти, если за заранее заданное время было совершено менее N_2 реагирований.
11. Способ по п.8, отличающийся тем, что если инцидент порожден не системным процессом, а операционная система хоста серверная то посредством модуля реагирования снимают содержимое оперативной памяти и останавливают процесс.
12. Способ по п.11, отличающийся тем, что снимают содержимое оперативной
10 памяти и останавливают процесс, если за заранее заданное время было совершено менее N_3 реагирований.
13. Способ по п.8, отличающийся тем, что если операционная система хоста не серверная, то посредством модуля реагирования изолируют от сети хост, на котором обнаружен инцидент.
14. Способ по п.13, отличающийся тем, что изолируют хост от сети, если за
15 заранее заданное время было изолированного менее N_4 хостов.
15. Способ по п. 1, отличающийся тем, что процесс автоматического реагирования, посредством модуля реагирования, осуществляют на уровне файла, на уровне хоста и на уровне корпоративной сети.
16. Способ по п. 15, отличающийся тем, что реагирование на уровне файла
20 включает в себя, полностью или частично, следующие шаги:
- блокируют по меньше мере один вредоносный файл и отправляют его в карантин;
 - отправляют по меньше мере один вредоносный файл на динамический анализ в изолированную среду;
 - 25 ищут по меньше мере один вредоносный файл, являющийся дочерним, на по меньшей мере одном хосте, и удаляют его;
 - завершают вредоносный процесс.
17. Способ по п. 15, отличающийся тем, что реагирование на уровне хоста включает в себя, полностью или частично, шаги, на которых:
- 30 собирают информацию об инциденте;
- создают копию содержимого оперативной памяти;
 - создают посекторную копию энергонезависимого запоминающего устройства;
 - изолируют хост от сети;
 - 35 блокируют запуск любых приложений, кроме оригинальных программ, разработанных производителем операционной системы.

18. Способ по п.17, отличающийся тем, что информация об инциденте включает в себя, по меньшей мере, сведения о программах, автоматически загружаемых при загрузке операционной системы, Prefetch-файлы, запущенные процессы, системные журналы событий, содержимое временных директорий.

5 19. Способ по п.15, отличающийся тем, что реагирование на уровне корпоративной сети включает в себя, полностью или частично, следующие шаги, на которых:

блокируют учетную запись пользователя;
запускают файлы сценария по работе с инцидентами;
10 отправляют отчет.

20. Система для принятия решения о необходимости автоматизированного реагирования на инцидент, состоящая из следующих функциональных модулей:

интерфейсный модуль, выполненный с возможностью получения от внешних систем сигналов об обнаружении инцидента;

15 аналитический модуль, выполненный с возможностью определять условия и выбирать способы автоматизированного реагирования;

модуль реагирования, выполненный с возможностью выполнения автоматизированного реагирования по пп. 1-19 вышеуказанного способа.

20

25

30

35