

СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ ИНФРАСТРУКТУРЫ ВРЕДОНОСНОЙ ПРОГРАММЫ ИЛИ КИБЕРЗЛОУМЫШЛЕННИКА

ОБЛАСТЬ ТЕХНИКИ

5 Настоящее техническое решение относится к области вычислительной техники, в частности, к способу и системе выявления инфраструктуры вредоносной программы или киберзлоумышленника.

УРОВЕНЬ ТЕХНИКИ

Из уровня техники известно решение RU2523114C2 (МПК G06F21/51, опубл.
10 20.07.2014), описывающее способ обнаружения узлов-посредников в вычислительной сети, через которое распространяется вредоносное ПО, при этом узлы-посредники подключены к сети Интернет, к которой также подключены вредоносные узлы. В данном способе используется комплекс вычислительных средств, сервисы выяснения маршрута следования трафика в сети, сервис WHOIS доступа к регистрационной информации о владельце домена
15 или IP-адреса с последующим построением графа распространения вредоносного ПО от вредоносного сайта по информационным каналам связи, выполняют оценку интенсивности использования канала связи для распространения вредоносного ПО, выявляют и блокируют промежуточный узел-посредник, используемый для неправомерных действий, дополнительно предусмотрена разблокировка узла-посредника, если со временем
20 значительно снижается интенсивность распространения вредоносного ПО или перестает представлять угрозу сайт, который непосредственно содержал вредоносное ПО. Данное решение осуществляет построение графов маршрутов трафика и ищет в нем вредоносных "посредников".

В заявленном решении не осуществляют анализ маршрутов трафика, а также сервис
25 WHOIS, Tracertroot используют только чтобы проверить связь с уже известными вредоносными узлами.

Из уровня техники известно решение US20080244744A1 (МПК G06F21/00, опубл.
02.10.2008), описывающее способ отслеживания трафика, поступающего на веб-сайт через сеть компьютеров, и идентификацию по меньшей мере одного правила из трафика,
30 подключенного к сети компьютеров, для определения вредоносного хоста, подключенного к сети компьютеров. Способ включает в себя ассоциирование первого IP-адреса и первого аппаратного отпечатка с утверждениями вредоносного хоста и сохранение информации, связанной с вредоносным хостом, по меньшей мере одной ячейке памяти базы данных. Способ также включает в себя идентификацию неизвестного хоста со второго веб-сайта,
35 определение второго IP-адреса и второго аппаратного отпечатка с неизвестным хостом и

определение, является ли неизвестный хост вредоносным хостом. Данное решение осуществляет мониторинг трафика и на выходе получают список вредоносных отпечатков, с которыми сравниваются новые хосты.

В заявленном решении не осуществляют анализ маршрутов трафика и на выходе получают правило. И именно в этом правиле основная ценность. Каждое новое правило позволит детектировать вредоносную инфраструктуру. Причём и ту, что работает сейчас, и ту, что работала год назад, а потом была выключена навсегда, и даже ту, что ещё не существует, а ещё только планируется злоумышленником (потому что он, собирая её, снова «засветит» свои предпочтения, которые учитывает правило).

Из уровня техники также известно решение RU2634209C1 (МПК G06F 21/55, опубл. 24.10.2017), описывающее способ автогенерации решающих правил для систем обнаружения вторжений с обратной связью, выполняемый на сервере. При этом способ включает, по крайней мере, следующие шаги: получают, по крайней мере, одно событие из базы данных событий, сформированной данными, полученными от, по крайней мере, одного сенсора; анализируют полученное, по крайней мере, одно событие на принадлежность к классу взаимодействия с центрами управления вредоносных программ; извлекают из, по крайней мере, одного вышеупомянутого события, относящегося к классу взаимодействия с центрами управления вредоносных программ, по крайней мере, один признак, используемый для формирования решающих правил; формируют решающие правила с использованием, по крайней мере, одного вышеупомянутого извлеченного признака; сохраняют сформированные решающие правила и предоставляют возможность получения обновления решающих правил для, по крайней мере, одного сенсора; сенсоры циклично проверяют доступность обновлений на центральном узле и при наличии обновлений получают их для использования, при этом в случае получения обновлений на сенсорах срабатывает триггер, осуществляющий перезагрузку решающих правил. Данное решение осуществляет формирование решающего правила по трафику и в нем ищет признаки вредоносных программ.

В заявленном решении, как уже указывалось выше, трафик совсем не анализируется и про признаки из трафика ничего не известно. Это самое важное отличие заявленного решения от известных из уровня техники.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Технической проблемой, на решение которой направлено заявленное техническое решение, является создание компьютерно-реализуемого способа и системы выявления инфраструктуры вредоносной программы или киберзлоумышленника, которые

охарактеризованы в независимых пунктах формулы. Дополнительные варианты реализации настоящего изобретения представлены в зависимых пунктах изобретения.

Технический результат заключается в повышение эффективности выявления компьютерных атак.

5 Заявленный результат достигается за счет осуществления компьютерно-реализуемого способа выявления инфраструктуры вредоносной программы или киберзлоумышленника, содержащий этапы, на которых:

- получают запрос, содержащий по меньшей мере один элемент инфраструктуры и тэг о принадлежности данного элемента вредоносной программе или киберзлоумышленнику;

- извлекают из базы данных по меньшей мере один параметр полученного элемента инфраструктуры, по меньшей мере один дополнительный элемент инфраструктуры, используемый той же вредоносной программой или киберзлоумышленником, что и полученный элемент инфраструктуры, и по меньшей мере один параметр по меньшей мере одного дополнительного элемента инфраструктуры;

- анализируют полученный по меньшей мере один элемент инфраструктуры и взаимосвязанный с ними по меньшей мере один параметр и дополнительный элемент инфраструктуры и взаимосвязанный с ним по меньшей мере один параметр;

- на основе анализа выявляют статистические связи между по меньшей мере одним параметром по меньшей мере одного полученного элемента инфраструктуры и по меньшей мере одним параметром по меньшей мере одного дополнительного элемента инфраструктуры;

- формируют правила поиска новых элементов инфраструктуры на основании выявленной статистической связи;

- извлекают, посредством сформированного правила, из базы данных новые элементы инфраструктуры;

- присваивают новым элементам тэги, соответствующие определенным вредоносным программам или киберзлоумышленникам, и сохраняют результаты в базе данных.

30 В частном варианте параметрами элементов инфраструктуры вредоносной программы или киберзлоумышленника является по меньшей мере одно из:

- i. IP-адрес;
- ii. доменное имя;
- iii. SSL-сертификат;
- iv. сервер;

- v. веб-сервис;
- vi. адрес электронной почты;
- vii. номер телефона.

В другом частном варианте базу данных постоянно пополняют данными, получаемыми при сканировании интернета.

В другом частном варианте сканирование интернета осуществляют посредством по меньшей мере одного сканера уязвимостей.

В другом частном варианте в качестве тэга используется условное или общепринятое название вредоносной программы или киберзлоумышленника.

В другом частном варианте запрос, содержащий по меньшей мере один элемент инфраструктуры, получают по меньшей мере из одного из следующих источников:

- i. «песочница»;
- ii. платформа детонации вредоносного ПО;
- iii. сканер уязвимостей;
- iv. honeypot;
- v. система обнаружения вторжений;
- vi. система быстрого реагирования на инциденты кибербезопасности.

В другом частном варианте выявление статистических связей выполняется с помощью алгоритмов машинного обучения.

В другом частном варианте статистическая связь представляет собой по меньшей мере два параметра, объединённые по меньшей мере одной логической операцией, причём каждый из параметров принадлежит по меньшей мере двум различным элементам инфраструктуры.

В другом частном варианте сформированные правила сохраняют и предоставляют возможность получения обновления правил.

Заявленный результат также достигается за счет системы выявления инфраструктуры вредоносной программы или киберзлоумышленника, включающая следующие модули:

модуль базы данных, выполненный с возможностью:

- хранения элементов инфраструктуры, параметров элементов инфраструктуры и тэгов о принадлежности данных элементов вредоносным программам или киберзлоумышленникам;

модуль обработки запросов, выполненный с возможностью:

- получения запроса, содержащего по меньшей мере один элемент инфраструктуры и тэг о принадлежности данного элемента вредоносной программе или киберзлоумышленнику;
- извлечения из запроса информацию об элементе инфраструктуры вредоносной программы или киберзлоумышленника, а также информацию о принадлежности данного элемента вредоносной программе или киберзлоумышленнику;
- модуль извлечения данных, выполненный с возможностью:
- получения от модуля обработки запросов по меньшей мере одного элемента инфраструктуры, принадлежащего вредоносной программе или киберзлоумышленнику, а также тэг о принадлежности данного элемента вредоносной программе или киберзлоумышленнику;
- извлечения из базы данных по меньшей мере одного параметра полученного элемента инфраструктуры, по меньшей мере одного дополнительного элемента инфраструктуры, используемого той же вредоносной программой или киберзлоумышленником, что и полученный элемент инфраструктуры, и по меньшей мере одного параметра по меньшей мере одного дополнительного элемента инфраструктуры;
- извлечения, посредством сформированного в аналитическом модуле правила, из базы данных новых элементы инфраструктуры;
- присвоения новым элементам тэги, соответствующие определенным вредоносным программам или киберзлоумышленникам, и сохранения результатов в базе данных;
- аналитический модуль, выполненный с возможностью:
- анализа, полученного по меньшей мере одного элемента инфраструктуры и взаимосвязанного с ними по меньшей мере одного параметра и дополнительного элемента инфраструктуры и взаимосвязанного с ним по меньшей мере одного параметра;
- на основе анализа выявления статистических связей между по меньшей мере одним параметром по меньшей мере одного полученного элемента инфраструктуры и по меньшей мере одним параметром по меньшей мере одного дополнительного элемента инфраструктуры;
- формирования правила поиска новых элементов инфраструктуры на основании выявленной статистической связи.

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 компьютерно-реализуемый способ выявления инфраструктуры вредоносной программы или киберзлоумышленника;

5 Фиг. 2 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
10 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 излишнее понимание особенностей настоящего изобретения.

Кроме того, из приведенного изложения будет ясно, что изобретение не
15 ограничивается приведенной реализацией. Многочисленные возможные модификации, изменения, вариации и замены, сохраняющие суть и форму настоящего изобретения, будут очевидными для квалифицированных в предметной области специалистов.

Ниже будут описаны термины и понятия, необходимые для осуществления настоящего технического решения.

20 **Под инфраструктурой вредоносной программы или киберзлоумышленника** понимаются используемые при работе вредоносной программы или деятельности киберзлоумышленника: IP-адреса, доменные имена, SSL-сертификаты, серверы (специализированное программное обеспечение) и веб-сервисы, адреса электронной почты, номера телефонов.

25 **Под параметрами элемента инфраструктуры** понимаются те параметры, которые присущи каждому элементу инфраструктуры данного типа. Например, параметрами, характеризующими такой элемент инфраструктуры, как веб-сервис, являются номер порта, на котором запущен данный сервис, дата и время его запуска, а также дата и время его остановки.

30 Некоторые параметры специфичны для элементов конкретного типа, как, например, название компании-регистратора является специфичным для параметра типа «доменное имя». Другие параметры могут быть сложными, то есть в свою очередь дополнительно характеризоваться несколькими параметрами. Так, например, такой специфичный параметр элемента «IP-адрес», как хостинг-провайдер, дополнительно характеризуется
35 географическим местонахождением, совокупностью веб-сервисов и серверов, доступных

клиентам хостинг-провайдера, диапазоном IP-адресов, принадлежащих данному хостинг-провайдеру и т.д.

Под статистической связью между элементами инфраструктуры понимается арифметическое, логическое или иное соответствие, позволяющее на основании известных соотношений между параметрами однотипных элементов инфраструктуры обнаружить в базе данных ещё один однотипный элемент инфраструктуры, одноимённые параметры которого связаны с параметрами известных элементов тем же соотношением.

Например, известны IP-адреса 11.22.33.44 и 55.66.77.88, выданные хостинг-провайдером Provider, LLC в один день, 11.11.2011, клиенту с контактным адресом client@mail.com и контактным номером телефона +1(099)100-100-10. Статистической связью между этими двумя IP-адресами и третьим IP-адресом 99.00.22.11, выданным в какой-то другой день, например, 12.12.2012, является то, что они выданы тем же хостинг-провайдером Provider, LLC клиенту с тем же контактным адресом client@mail.com, но другим контактным номером телефона +1(059)200-200-20.

Под правилом поиска новых элементов инфраструктуры понимается решающее правило, способное отобрать в базе данных известной структуры те вхождения, которые удовлетворяют заданным условиям, например, все IP-адреса, выданные указанным хостинг-провайдером в один день. Правило может быть реализовано как скрипт, регулярное выражение, как классификатор, обученный средствами машинного обучения, и т.д. Настоящее изобретение направлено на обеспечение компьютерно-реализуемого способа и системы выявления инфраструктуры вредоносной программы или киберзлоумышленника.

Как представлено на Фиг. 1, заявленный компьютерно-реализуемый способ выявления инфраструктуры вредоносной программы или киберзлоумышленника (100) реализован следующим образом:

На этапе (101) получают запрос, содержащий по меньшей мере один элемент инфраструктуры и тэг о принадлежности данного элемента вредоносной программе или киберзлоумышленнику.

Элементами инфраструктуры могут быть, например, IP-адрес, доменное имя, SSL-сертификат, сервер, веб-сервис, адрес электронной почты, номер телефона. В качестве информации о принадлежности данного элемента к вредоносной программе или киберзлоумышленнику может использоваться условное или общепринятое название вредоносной программы или киберзлоумышленника, например, вредоносная программа Zeus.

Указанная выше информация поступает в модуль обработки запросов, выполненный с возможностью извлечения такой информации. Модуль обработки запросов связывается с источниками запросов, от которых такие запросы поступают, по проводной и/или беспроводной связи.

5 Источниками входящих запросов могут являться, например, но не ограничиваясь, «песочница» (специально выделенная среда для безопасного исполнения программ) или платформа детонации вредоносного ПО, сканер уязвимостей, honeypot (ресурс-приманка для киберзлоумышленника) различных разновидностей, система обнаружения вторжений, система быстрого реагирования на инциденты кибербезопасности.

10 Именно посредством сканера уязвимостей осуществляется снятие отпечатков с сервисов, поднятых на портах удалённых серверов. Собственно, сканер уязвимостей может быть реализован любым общеизвестным образом.

Все перечисленные программы и системы могут располагаться как внутри одной интранет-сети с системой, реализующей способ, так и на удалённых серверах, с
15 обеспечением связи между ними по интернету.

Также источниками запросов могут быть системы центров быстрого реагирования на инциденты кибербезопасности, CERT (Computer Emergency Response Team), автоматически сообщающие о вредоносной активности в контролируемых сетях, удалённые компьютеры, владельцы которых присылают на указанный адрес электронной
20 почты сведения об обнаружении на их компьютере вредоносных программ, мобильные телефоны, владельцы которых присылают на указанный для связи номер SMS или MMS, содержащие сведения о работе вредоносной программы и т.д.

Также источником входящих запросов может быть оператор системы, получающий соответствующую информацию по телефону или электронной почте и вводящий её в
25 интерфейсе модуля обработки входящих запросов.

Модуль обработки запросов извлекает из запроса информацию об элементе инфраструктуры вредоносной программы или киберзлоумышленника, а также информацию о принадлежности элемента, и передаёт её модулю извлечения данных. Например, от «песочницы» поступил запрос, содержащий информацию о том, что
30 вредоносная программа Zeus отправляет данные с зараженного компьютера на сервер с доменом bad-domain.com, причём у этого домена текущий IP-адрес 11.22.33.44. Модуль обработки запросов извлекает из запроса перечисленную информацию и передаёт модулю извлечения данных доменное имя bad-domain.com, снабжённое тэгом Zeus и IP-адрес 11.22.33.44, снабжённый тэгом Zeus. На этом первый этап завершается.

Далее на этапе (102) извлекают из базы данных по меньшей мере один параметр полученного элемента инфраструктуры, по меньшей мере один дополнительный элемент инфраструктуры, используемый той же вредоносной программой или киберзлоумышленником, что и полученный элемент инфраструктуры, и по меньшей мере

5 один параметр по меньшей мере одного дополнительного элемента инфраструктуры.

Модуль извлечения данных, выполненный с возможностью связи с модулем обработки запросов, с аналитическим модулем и с базой данных, получает от модуля обработки запросов по меньшей мере один элемент инфраструктуры, принадлежащий вредоносной программе или киберзлоумышленнику, а также информацию о

10 принадлежности данного элемента определённой программе или киберзлоумышленнику (тэг).

Модуль извлечения данных выполняет поиск в базе данных всех записей, содержащих данный элемент инфраструктуры, а также данный тэг.

База данных, а также поиск в ней могут быть реализованы любым известным

15 образом, например, так, как это описано в патенте RU2681699. Аналогично описанному в патенте способу, информация в базе данных может быть структурирована в виде таблицы, демонстрирующей взаимосвязь между, по меньшей мере, следующими параметрами таким образом, что каждому элементу инфраструктуры, например, доменному имени, соответствует, например, по меньшей мере один из следующих параметров: тэг, IP-адрес,

20 SSL-ключ, SSH-отпечаток, список работающих сервисов, история работающих сервисов, история доменных имен, история IP-адресов, история DNS-серверов, история владельцев доменного имени или IP-адреса.

Параметры также могут включать ресурсные записи DNS, которые представляют собой записи о соответствии имени и служебной информации в системе доменных имен.

25 Данные могут храниться в одной или нескольких базах либо таблицах. В целом поиск осуществляется традиционными способами: одним или многими запросами к этим базам/таблицам и поиском пересечений между результатами.

Например, в результате поиска доменного имени bad-domain.com в базе данных ничего не найдено, в ходе поиска адреса IP-адреса 11.22.33.44 в базе данных ничего не

30 найдено, а в ходе поиска тэга Zeus в базе данных найден IP-адрес 55.66.77.88, также помеченный ранее этим тэгом.

На этом данный этап завершается, и модуль извлечения данных переходит к выполнению следующего этапа.

Модуль извлечения данных извлекает из базы данных все параметры, имеющие

35 взаимосвязь с найденными в базе данных элементами инфраструктуры.

В рассматриваемом примере для найденного в базе данных IP-адреса 55.66.77.88 будут, например, извлечены: доменное имя another-bad-domain.net, название владельца данного IP-адреса - Provider, LLC, название регистратора данного доменного имени - Registrar, LLC, дата выдачи данного IP-адреса - 11.11.2011, дата регистрации данного доменного имени - 22.12.2011, контактный адрес электронной почты клиента, которому был выдан данный IP-адрес - client@mail.com и контактный номер телефона клиента: +1(099)100-100-10.

Если какие-либо элементы инфраструктуры не были найдены в базе данных на втором этапе, то модуль извлечения данных извлекает параметры, ассоциированные с такими элементами инфраструктуры, из доступных онлайн-источников. Это может быть выполнено при помощи, например, онлайн-службы «Whois» или любой известной программы соответствующего назначения, например, программы «nslookup».

В этом случае модуль извлечения данных может, например, автоматически направлять соответствующий поисковый запрос в онлайн-службу «Whois» и извлекать необходимые сведения из ответа онлайн-службы «Whois» или из веб-страницы с результатами выполнения поискового запроса. Последнее может быть выполнено путем использования, например, специального парсера, встроенного в модуль извлечения данных и анализирующего, например, текст ответа онлайн-службы «Whois» или html-код указанной веб-страницы.

В данном примере описанным образом для IP-адреса 11.22.33.44 и доменного имени bad-domain.com могут быть извлечены: название владельца данного IP-адреса - Provider, LLC, название регистратора данного доменного имени -- AnotherRegistrar, LLC, дата выдачи данного IP-адреса - 11.11.2011, дата регистрации данного доменного имени - 23.12.2011, контактный адрес электронной почты клиента, которому был выдан данный IP-адрес - anotherclient@mail.com и контактный номер телефона клиента: +1(099)300-300-30.

Эти параметры модуль извлечения данных сохраняет в базе данных с сохранением указания на взаимосвязь между названными параметрами, IP-адресом 11.22.33.44, доменным именем bad-domain.com, тэгом Zeus, а также датой поступления указанных элементов инфраструктуры и источника, из которого они поступили (в данном случае – идентификатора той «песочницы», где в рассматриваемом примере была обнаружена активность вредоносной программы Zeus).

Затем модуль извлечения данных передает аналитическому модулю найденные элементы инфраструктуры и взаимосвязанные с ними параметры.

И на этапе (103) анализируют полученный по меньшей мере один элемент инфраструктуры и взаимосвязанный с ними по меньшей мере один параметр и

дополнительный элемент инфраструктуры и взаимосвязанный с ним по меньшей мере один параметр.

В данном примере аналитическому модулю будут переданы доменные имена bad-domain.com и another-bad-domain.net, IP-адреса 11.22.33.44 и 55.66.77.88, названия владельцев данного IP-адреса (в нашем примере они совпадают), названия регистраторов доменного имени -- Registrar, LLC и AnotherRegistrar, LLC, даты выдачи каждого IP-адреса (в нашем примере это одна дата), даты регистрации каждого доменного имени, 22.12.2011 и 23.12.2011, контактные адреса электронной почты клиента, контактные номера телефонов, а также тэг Zeus. На этом выполнение данного этапа завершается.

На этапе (104) на основе анализа выявляют статистические связи между по меньшей мере одним параметром по меньшей мере одного полученного элемента инфраструктуры и по меньшей мере одним параметром по меньшей мере одного дополнительного элемента инфраструктуры.

Аналитический модуль, выполненный с возможностью связи с модулем извлечения данных и модулем построения правил, получает от модуля извлечения данных элементы инфраструктуры и взаимосвязанные с ними параметры.

На основании этих данных аналитический модуль выстраивает статистические связи, то есть арифметические, логические или иные соответствия, позволяющее на основании известных соотношений между параметрами однотипных элементов инфраструктуры обнаружить в базе данных ещё как минимум один однотипный элемент инфраструктуры, одноимённые параметры которого связаны с параметрами известных элементов тем же самым соотношением.

Например, аналитический модуль обнаружит, что:

- у полученных IP-адресов один и тот же владелец, Provider, LLC,
- оба IP-адреса выданы в один и тот же день, 11.11.2011,
- контактные адреса электронной почты клиента, хотя и принадлежат разным учётным записям, client@mail.com и anotherclient@mail.com, зарегистрированы на одном и том же почтовом сервере mail.com.

Соответственно, выявленная статистическая связь, в данном примере, может быть записана следующим простым логическим выражением:

ВЛАДЕЛЕЦ_IP-АДРЕСА="Provider,LLC" _Λ_ ДЕНЬ_ВЫДАЧИ_IP-АДРЕСА="11.11.2011" _Λ_ EMAIL_КЛИЕНТА="*@mail.com",

где Λ - оператор конъюнкции, логическое «И», * - так называемый символ-джокер, означающий, что на его месте может быть любое количество любых символов, идущих подряд без пробела.

В дальнейшем под признаками статистической связи будут пониматься те элементы инфраструктуры или параметры элементов инфраструктуры, сочетание которых позволяет построить выявленную статистическую связь.

В вышеприведённом примере это название компании-владельца (провайдера) IP-адресов, день выдачи IP-адреса и часть адреса электронной почты клиента.

Приведённый пример достаточно прост сам по себе, в более сложном примере аналитическому модулю может быть передан для анализа список из нескольких сотен IP-адресов, зарегистрированных в разное время у разных провайдеров и не связанных с повторяющимися или похожими доменными именами, а также взаимосвязанный с каждым из этих IP-адресов список работающих сервисов и список истории работающих сервисов. В ходе анализа подобных данных аналитическим модулем может быть выявлена более сложная статистическая связь. Например, может быть выявлен тот факт, что на каждом из этих IP-адресов по крайней мере один раз был запущен HTTP-сервер Apache, который проработал 48 часов и был остановлен, а сразу же после его останова на том же IP-адресе был запущен e-mail сервер CommuniGate Pro версии 5.1 с поддержкой API-интерфейса XIMSS.

Описанное выявление статистических связей может выполняться с помощью алгоритмов машинного обучения.

После выявления всех статистических связей выполнение данного этапа завершается, и аналитический модуль переходит к выполнению следующего этапа. Также в одной из возможных альтернативных реализаций аналитический модуль может передавать модулю извлечения данных сведения о выявленной статистической связи.

На этапе (105) формируют правила поиска новых элементов инфраструктуры на основании выявленной статистической связи.

На данном этапе аналитический модуль строит, на основании выявленных признаков статистических связей, правило поиска новых элементов инфраструктуры.

В альтернативном варианте реализации новое правило поиска элементов инфраструктуры строит модуль извлечения данных на основании сведений о выявленных статистических связях, полученных от аналитического модуля.

В основе правила лежит набор признаков, применительно к которым на предыдущем этапе было обнаружено, что совокупно они составляют выявленную статистическую связь. Само по себе правило представляет собой такой набор признаков, описанных на некотором формальном псевдоязыке.

В качестве неограничивающих примеров формального псевдоязыка могут быть названы SQL, Python и т.д.

Данные, как было отмечено выше, могут храниться в одной или нескольких базах/таблицах. Поиск осуществляется одним или многими запросами к этим базам/таблицам и поиском пересечений между результатами.

Если правило написано на один признак, например, на отпечаток специфического сервиса, такого как e-mail сервер CommuniGate Pro версии 5.1, то поиск будет проходить по одной базе/таблице, в которой хранятся именно отпечатки различных сервисов.

Если правило сложное и содержит признаки доменов, сертификатов, и так далее, то запросы будут делаться к разным базам/таблицам и потом будут искаться пересечения между результатами.

Например, по сложному правилу может проводиться поиск всех доменов, зарегистрированных регистратором AAAA, у каждого из которых (доменов) имеется сертификат, выпущенный компанией BBBB, а также у каждого из которых (доменов) когда-либо существовал IP-адрес, на котором когда-либо был запущен HTTP-сервер Apache.

Новое правило аналитический модуль передаёт модулю извлечения данных, и на этом выполнение данного этапа завершается.

В том случае, если новое правило поиска элементов инфраструктуры строил модуль извлечения данных, он непосредственно переходит к выполнению следующего этапа.

На этапе (106) извлекают, посредством сформированного правила, из базы данных новые элементы инфраструктуры.

Модуль извлечения данных выполняет поиск в базе данных всех записей, удовлетворяющих условиям, описанным новым правилом поиска.

В рассматриваемом примере, в результате поиска в базе данных может быть обнаружен новый IP-адрес 99.00.22.11, не имеющий тэга Zeus, но выданный тем же хостинг-провайдером Provider, LLC, клиенту с контактным адресом thirdclient@mail.com в тот же день 11.11.2011, что и предыдущие два IP-адреса, отмеченные тэгом Zeus.

На этом выполнение данного этапа завершается.

На этапе (107) присваивают новым элементам тэги, соответствующие определенным вредоносным программам или киберзлоумышленникам, и сохраняют результаты в базе данных.

В этом случае модуль извлечения данных присваивает найденному IP-адресу 99.00.22.11 тэг Zeus и сохраняет результат в базе данных. Таким образом оказывается обнаружен новый элемент инфраструктуры, используемый данной вредоносной программой.

Следует отметить, что подобный алгоритм позволяет обнаружить «спящие», то есть уже созданные, но пока до сих пор ни разу не использовавшиеся элементы инфраструктуры вредоносных программ или киберзлоумышленников.

В представленном примере, найденный IP-адрес 99.00.22.11 и связанное с ним доменное имя могли быть заблаговременно созданы разработчиками вредоносной программы Zeus, однако до описанного момента остаются не обнаруженными какими-либо средствами обеспечения кибербезопасности, поскольку вредоносная программа ещё ни разу не обращалась к этому серверу.

Вне прямой связи с вышеописанными шагами также постоянно ведётся пополнение базы данных, упомянутой выше. Для пополнения выполняются следующие действия.

Постоянно осуществляют сканирование интернета и снимают отпечатки запущенных сервисов на открытых портах. Вместе с этим собирают данные о доменах, которые связаны с найденными серверами.

Снятие отпечатков с сервисов, запущенных на портах удалённых серверов, выполняется посредством сканера уязвимостей, который может быть реализован любым общеизвестным образом.

Результаты сканирования упорядочиваются и помещаются в базу данных.

На Фиг. 2 далее будет представлена общая схема компьютерного устройства (200), обеспечивающего обработку данных, необходимую для реализации заявленного решения.

В общем случае устройство (200) содержит такие компоненты, как: один или более процессоров (201), по меньшей мере одну память (202), средство хранения данных (203), интерфейсы ввода/вывода (204), средство В/В (205), средства сетевого взаимодействия (206).

Процессор (201) устройства выполняет основные вычислительные операции, необходимые для функционирования устройства (200) или функциональности одного или более его компонентов. Процессор (201) исполняет необходимые машиночитаемые команды, содержащиеся в оперативной памяти (202).

Память (202), как правило, выполнена в виде ОЗУ и содержит необходимую программную логику, обеспечивающую требуемый функционал.

Средство хранения данных (203) 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 (203) позволяет выполнять долгосрочное хранение различного вида информации, например, вышеупомянутых файлов с наборами данных пользователей, базы данных, содержащих записи измеренных для каждого пользователя временных интервалов, идентификаторов пользователей и т.п.

Интерфейсы (204) 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 (204) зависит от конкретного исполнения устройства (N00),
5 которое может представлять собой персональный компьютер, мейнфрейм, серверный кластер, тонкий клиент, смартфон, ноутбук и т.п.

В качестве средств В/В данных (205) в любом воплощении системы, реализующей описываемый способ, должна использоваться клавиатура. Аппаратное исполнение клавиатуры может быть любым известным: это может быть, как встроенная клавиатура,
10 используемая на ноутбуке или нетбуке, так и обособленное устройство, подключенное к настольному компьютеру, серверу или иному компьютерному устройству. Подключение при этом может быть, как проводным, при котором соединительный кабель клавиатуры подключен к порту PS/2 или USB, расположенному на системном блоке настольного компьютера, так и беспроводным, при котором клавиатура осуществляет обмен данными
15 по каналу беспроводной связи, например, радиоканалу, с базовой станцией, которая, в свою очередь, непосредственно подключена к системному блоку, например, к одному из USB-портов. Помимо клавиатуры, в составе средств В/В данных также может использоваться: джойстик, дисплей (сенсорный дисплей), проектор, тачпад, манипулятор мышь, трекбол, световое перо, динамики, микрофон и т.п.

Средства сетевого взаимодействия (206) 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 (205) обеспечивается организация обмена данными по проводному или беспроводному каналу передачи данных, например, WAN, PAN, ЛВС (LAN), Интранет,
25 Интернет, WLAN, WMAN или GSM.

Компоненты устройства (200) сопряжены посредством общей шины передачи данных (210).

В настоящих материалах заявки было представлено предпочтительное раскрытие осуществление заявленного технического решения, которое не должно использоваться как
30 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 изобретения

1. Компьютерно-реализуемый способ выявления инфраструктуры вредоносной программы или киберзлоумышленника, содержащий этапы, на которых:

- получают запрос, содержащий по меньшей мере один элемент инфраструктуры и тэг о принадлежности данного элемента вредоносной программе или киберзлоумышленнику;
- извлекают из базы данных по меньшей мере один параметр полученного элемента инфраструктуры, по меньшей мере один дополнительный элемент инфраструктуры, используемый той же вредоносной программой или киберзлоумышленником, что и полученный элемент инфраструктуры, и по меньшей мере один параметр по меньшей мере одного дополнительного элемента инфраструктуры;
- анализируют полученный по меньшей мере один элемент инфраструктуры и взаимосвязанный с ними по меньшей мере один параметр и дополнительный элемент инфраструктуры и взаимосвязанный с ним по меньшей мере один параметр;
- на основе анализа выявляют статистические связи между по меньшей мере одним параметром по меньшей мере одного полученного элемента инфраструктуры и по меньшей мере одним параметром по меньшей мере одного дополнительного элемента инфраструктуры;
- формируют правила поиска новых элементов инфраструктуры на основании выявленной статистической связи;
- извлекают, посредством сформированного правила, из базы данных новые элементы инфраструктуры;
- присваивают новым элементам тэги, соответствующие определенным вредоносным программам или киберзлоумышленникам, и сохраняют результаты в базе данных.

2. Способ по п.1, характеризующийся тем, что параметрами элементов инфраструктуры вредоносной программы или киберзлоумышленника является по меньшей мере одно из:

- i. IP-адрес;
- ii. доменное имя;
- iii. SSL-сертификат;
- iv. сервер;
- v. веб-сервис;
- vi. адрес электронной почты;
- vii. номер телефона.

3. Способ по п.1, характеризующийся тем, что базу данных постоянно пополняют данными, получаемыми при сканировании интернета.

4. Способ по п.3, характеризующийся тем, что сканирование интернета осуществляют посредством по меньшей мере одного сканера уязвимостей.

5 5. Способ по п.1, характеризующийся тем, что в качестве тэга используется условное или общепринятое название вредоносной программы или киберзлоумышленника.

6. Способ по п.1, характеризующийся тем, что запрос, содержащий по меньшей мере один элемент инфраструктуры, получают по меньшей мере из одного из следующих источников:

10 i. «песочница»;

ii. платформа детонации вредоносного ПО;

iii. сканер уязвимостей;

iv. honeypot;

v. система обнаружения вторжений;

15 vi. система быстрого реагирования на инциденты кибербезопасности

7. Способ по п.1, характеризующийся тем, что выявление статистических связей выполняется с помощью алгоритмов машинного обучения.

8. Способ по п.1, характеризующийся тем, что статистическая связь представляет собой по меньшей мере два параметра, объединённые по меньшей мере одной логической операцией, причём каждый из параметров принадлежит по меньшей мере двум различным элементам инфраструктуры.

20

9. Способ по п.1, характеризующийся тем, что сформированные правила сохраняют и предоставляют возможность получения обновления правил.

10. Система выявления инфраструктуры вредоносной программы или киберзлоумышленника, включающая следующие модули:

25

модуль базы данных, выполненный с возможностью:

- хранения элементов инфраструктуры, параметров элементов инфраструктуры и тэгов о принадлежности данных элементов вредоносным программам или киберзлоумышленникам;

30 модуль обработки запросов, выполненный с возможностью:

- получения запроса, содержащего по меньшей мере один элемент инфраструктуры и тэг о принадлежности данного элемента вредоносной программе или киберзлоумышленнику;

- извлечения из запроса информацию об элементе инфраструктуры вредоносной программы или киберзлоумышленника, а также информацию о принадлежности данного элемента вредоносной программе или киберзлоумышленнику;

модуль извлечения данных, выполненный с возможностью:

5 • получения от модуля обработки запросов по меньшей мере одного элемента инфраструктуры, принадлежащего вредоносной программе или киберзлоумышленнику, а также тэг о принадлежности данного элемента вредоносной программе или киберзлоумышленнику;

10 • извлечения из базы данных по меньшей мере одного параметра полученного элемента инфраструктуры, по меньшей мере одного дополнительного элемента инфраструктуры, используемого той же вредоносной программой или киберзлоумышленником, что и полученный элемент инфраструктуры, и по меньшей мере одного параметра по меньшей мере одного дополнительного элемента инфраструктуры;

15 • извлечения, посредством сформированного в аналитическом модуле правила, из базы данных новых элементы инфраструктуры;

- присвоения новым элементам тэги, соответствующие определенным вредоносным программам или киберзлоумышленникам, и сохранения результатов в базе данных;

аналитический модуль, выполненный с возможностью:

20 • анализа, полученного по меньшей мере одного элемента инфраструктуры и взаимосвязанного с ними по меньшей мере одного параметра и дополнительного элемента инфраструктуры и взаимосвязанного с ним по меньшей мере одного параметра;

25 • на основе анализа выявления статистических связей между по меньшей мере одним параметром по меньшей мере одного полученного элемента инфраструктуры и по меньшей мере одним параметром по меньшей мере одного дополнительного элемента инфраструктуры;

- формирования правила поиска новых элементов инфраструктуры на основании выявленной статистической связи.

30

35