Sandbox версия 5.7

Руководство пользователя

Дата редакции документа: 18.01.2024

Содержание

1. Об этом документе

Руководство пользователя содержит пошаговые инструкции по отправке файлов на проверку в Positive Technologies Sandbox (далее также — PT Sandbox) через интерфейс продукта или по электронной почте и просмотру результатов проверки. Руководство не содержит инструкции по установке, первоначальной настройке и администрированию PT Sandbox.

Руководство адресовано всем сотрудникам организации, использующей PT Sandbox в своей информационной системе.

Комплект документации PT Sandbox включает в себя следующие документы:

- Этот документ.
- Руководство администратора — содержит справочную информацию и инструкции по установке, настройке и администрированию продукта.
- Руководство специалиста по безопасности — содержит сценарии использования продукта для управления событиями информационной безопасности.
- Руководство разработчика — содержит информацию для интеграции PT Sandbox со сторонними системами.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о PT Sandbox (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом

Пример	Описание
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT Sandbox

Вы можете найти дополнительную информацию о PT Sandbox на портале технической поддержки.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 13).

2. О PT Sandbox

Positive Technologies Sandbox (PT Sandbox) — это программный комплекс, предназначенный для проверки файлов и электронных писем на предмет угрозы информационной безопасности. С помощью PT Sandbox пользователи и специалисты по безопасности могут получить оценку опасности, исходящей от файлов и электронных писем, поступающих в информационную систему извне, отправляемых за ее пределы или уже находящихся внутри нее.

Функции PT Sandbox:

— проверка файлов с помощью методов поведенческого и статического анализа;

— проверка файлов, поступающих в информационную систему извне, отправляемых за ее пределы или уже находящихся внутри нее;

— недопуск в информационную систему файлов и электронных писем, которые по результатам проверки представляют угрозу;

— создание в интерфейсе PT Sandbox графических отчетов о результатах проверки.

PT Sandbox позволяет вам:

— самостоятельно отправлять файлы на проверку через интерфейс PT Sandbox;

— отправлять файлы на проверку во вложениях электронных писем на специальный адрес электронной почты и получать результаты проверки в ответном письме;

— проверять ссылки, ведущие на файлы;

— просматривать результаты проверки файлов.

3. Что нового в версии 5.7

Ниже приводится список изменений, которые появились в PT Sandbox.

Фильтрация извлеченных ссылок при проверке файлов через веб-интерфейс

Теперь при проверке файлов через веб-интерфейс вы можете настроить фильтрацию извлеченных из файлов ссылок. PT Sandbox скачивает и проверяет контент только по тем ссылкам, которые удовлетворяют указанным вами параметрам. Вы можете указать адреса, с которых будет скачиваться контент для проверки, и исключаемые адреса. Также вы можете включить эвристику для обнаружения и проверки подозрительных ссылок и ограничить количество проверяемых ссылок в одном задании.

Определение некоторых типов файлов офисных форматов как потенциально опасных

Теперь PT Sandbox относит к потенциально опасным файлы Microsoft Office версии 2007 и выше, если они используют элементы ActiveX, содержат запросы к внешним данным, используют шаблон, функции динамического обмена данными (DDE) или содержат настроенные действия (Actions). Вы можете изменить такое поведение, изменив критерии определения потенциально опасных файлов в параметрах проверки.

Распаковка ELF-файлов, сжатых приложением UPX

Исполняемые файлы ELF могут быть сжаты с помощью приложения UPX для защиты и уменьшения их объема. Теперь при статическом анализе PT Sandbox может распаковывать и проверять такие файлы.

Фильтрация объектов в таблице с угрозами в карточке задания

В карточке задания изменена таблица с угрозами. Теперь вы можете скрыть объекты с угрозами, которые унаследовали свой вердикт от дочерних, и просматривать только те объекты, которые стали причиной вердикта и содержат вредоносное ПО (в таблице не отображаются артефакты поведенческого анализа). По значку ⓘ вы можете посмотреть, какими средствами проверки угрозы были обнаружены. Также теперь в таблице вы можете просматривать все объекты задания или только объекты первого уровня вложенности.

4. Принципы работы и особенности использования PT Sandbox

Раздел содержит основную информацию о принципах работы и особенностях использования PT Sandbox.

В этом разделе

4.1. Безопасность данных при передаче и обработке

При работе с интерфейсом все передаваемые данные защищаются при помощи HTTPS с использованием SSL-сертификата. SSL-сертификат может быть как самоподписанным, так и выданным официальным центром сертификации.

Любые файлы, скачиваемые специалистом по безопасности из хранилища файлов, помещаются в ZIP-архивы с паролем infected.

При взаимодействии PT Sandbox с сервисом управления пользователями и доступом PT Management and Configuration (PT MC) все данные передаются в зашифрованном виде.

4.2. Алгоритм работы PT Sandbox

Проверка объектов в PT Sandbox выполняется согласно следующему алгоритму:

1. Объект поступает на проверку в PT Sandbox от одного из настроенных источников или через веб-интерфейс. Для объекта создается задание на проверку, карточка задания. В карточку задания добавляется карточка исходного объекта.
2. Выполняются определение типа объекта и выделение дочерних объектов:
   - Если объект является письмом, из него выделяются тело письма, файлы вложений, выполняется поиск ссылок и скачивание файлов по этим ссылкам.
   - Если объект является архивом, выполняется декомпрессия или распаковка файлов. Для зашифрованных архивов выполняется подбор пароля.
   - Если объект является ссылкой, скачивается файл по этой ссылке.

В карточку задания добавляются отдельные карточки для объектов, связанных с исходным объектом.

3. Собираются данные об объектах задания и заносятся в карточки объектов. Например, для файла указываются хеш-суммы (MD5, SHA-1 и SHA-256), размер и MIME-тип.
4. Каждый объект задания проверяется с помощью различных методов проверки в соответствии с заданными параметрами проверки, результаты проверок заносятся в карточку объекта. На основании результатов проверок принимается решении о наличии или отсутствии угрозы в объекте — выносится вердикт по объекту.
5. На основании вердиктов по отдельным объектам выносится вердикт о наличии или отсутствии угрозы в исходном объекте, поступившем на проверку.
6. Файлы задания сохраняются в хранилище файлов. Извлеченные из архивов файлы и вложения электронных писем сохраняются в хранилище как отдельные файлы. Если файл имеет размер больше 1 ГБ или занимает больше 1% от объема хранилища, он удаляется.
7. Если для источника настроен блокирующий режим работы, в зависимости от вердикта проверенный файл или электронное письмо пропускается в информационную систему или блокируется.

4.3. Методы проверки объектов

Для получения информации об опасности объектов PT Sandbox проверяет их методами статического и динамического анализа.

Статический анализ

К статическому анализу относятся следующие методы проверки:

— Антивирусное сканирование файлов. Проверка файлов в многопоточном режиме с помощью антивирусов сторонних разработчиков.

— Экспертная оценка файлов. Проверка файлов с помощью YARA-правил из базы знаний средства проверки PT ESC, разработанного специалистами экспертного центра Positive Technologies.

— Проверка файлов по спискам. Проверка хеш-сумм файлов по черному и белому спискам, составленным специалистами по информационной безопасности вашей организации.

— Проверка файлов и ссылок по индикаторам компрометации с помощью средства проверки PT IoC. Индикатор компрометации — это объект или свойство объекта, которые указывают на подозрительную или вредоносную активность в информационной системе. Индикаторами компрометации для файлов могут быть хеш-суммы, для ссылок — URL, IP-адреса и имена доменов.

— Ретроспективный анализ файлов. Регулярная повторная проверка файлов из хранилища с использованием обновленных антивирусных баз и обновленной базы знаний средства проверки PT ESC.

Динамический анализ

К динамическому анализу относятся следующие методы проверки:

— Поведенческий анализ файлов. Анализ поведения файлов в изолированной виртуальной среде.

  Файл запускается в специально подготовленном образе ОС, в котором анализируется его поведение. Образ может содержать специальные файлы-приманки, которые выглядят привлекательной мишенью и провоцируют вредоносное ПО на попытки получить к ним доступ. При этом отслеживаются следующие действия файла: создание файлов (артефактов), запуск процессов, выполнение интернет-запросов, изменение оперативной памяти, изменение системного реестра.

  Для выявления вредоносного ПО используются правила из базы знаний экспертного центра Positive Technologies. Эти правила определяют признаки опасного и потенциально опасного поведения файла. Все полученные в ходе анализа артефакты сохраняются в хранилище файлов и проверяются методами статического анализа.

— Анализ файлов с использованием машинного обучения. Анализ поведения файлов в изолированной виртуальной среде с помощью средства проверки PT ML, разработанного специалистами экспертного центра Positive Technologies на основе технологии машинного обучения.

— Анализ ссылок. Поиск и скачивание контента по ссылкам с помощью средства проверки PT Crawler и механизма curl. Скачанные файлы сохраняются в хранилище файлов и проверяются методами статического анализа.

4.4. Особенности работы с архивами

PT Sandbox извлекает файлы из архивов форматов 7Z, ACE, ARJ, BZ2, CAB, GZ, ISO, LZ, LZMA, OneNote (с расширением .one), RAR, TAR (.tar, .tar.bz2, .tar.gz, .tar.lzma, .tar.xz), XZ, Z, ZIP.

Для проверки зашифрованного архива необходим пароль. В PT Sandbox существует список стандартных паролей, который задается сотрудниками службы информационной безопасности. Если вы загружаете архив, зашифрованный нестандартным паролем, вы можете ввести этот пароль при загрузке файла через интерфейс или в теле письма при отправке файла по электронной почте. Архивы, которые PT Sandbox не может расшифровать, не проверяются и сохраняются в хранилище файлов без распаковки.

При распаковке архивов форматов CAB и ISO в структуре задания отображается архив и все вложенные в него файлы. Архив и все вложенные файлы проверяются с помощью антивирусов и правил PT ESC. Вложенные файлы проверяются с помощью поведенческого анализа.

При распаковке архивов формата MSI в структуре задания архив отображается без вложенных файлов. Архив проверяется с помощью антивирусов, правил PT ESC и поведенческого анализа. Вложенные файлы проверяются с помощью правил PT ESC.

4.5. Особенности работы со сжатыми файлами

Перед проверкой сжатого файла PT Sandbox может выполнять его декомпрессию. PT Sandbox поддерживает несколько методов сжатия.

Таблица 2. Поддерживаемые методы сжатия файлов

Метод сжатия	Расширения файлов
gzip	.gz
compress	.z
bzip2	.bz2
LZMA	.lz, .lzma
LZMA2	.xz

4.6. Особенности проверки электронных писем

PT Sandbox проверяет электронные письма форматов EML, MSG и TNEF. При проверке PT Sandbox выделяет почтовые заголовки, текст письма и вложения для анализа экспертными правилами PT ESC.

Для электронного письма, полученного от почтового источника, в списке заданий отображается своя строка. Извлеченные из письма вложения отображаются в задании как дочерние элементы к этому письму.

4.7. Особенности проверки ссылок

PT Sandbox проверяет ссылки, отправленные через веб-интерфейс и извлеченные из электронных писем от источников. Ссылки извлекаются из писем форматов HTML, RTF, TXT и их вложений. Из вложений форматов HTML, RTF извлекаются ссылки, добавленные в виде простого текста, и ссылки, выделенные специальными тегами (в соответствии с форматом вложения). Из вложений форматов DOCX, PDF, PPTX, XLSX извлекаются только выделенные тегами ссылки. Все ссылки проверяются по индикаторам компрометации. Также PT Sandbox может скачивать по ссылкам файлы и проверять их всеми доступными средствами проверки.

PT Sandbox сохраняет информацию о проверенных ссылках: адрес, статус проверки, результат проверки, дату и время проверки ссылки, информацию о скачанном по ссылке файле, серию переадресаций.

5. Требования к рабочим станциям

Для узла, с которого выполняется вход в веб-интерфейс PT Sandbox, выдвигаются следующие аппаратные и программные требования:

— Разрешение монитора —Full HD (не менее 1920 × 1080 пикселей).

— Браузер — Google Chrome версии 49 и выше или Mozilla Firefox версии 45 и выше.

— На рабочей станции администратора должны быть разрешены исходящие подключения к порту TCP 22.

— Если на узле установлен антивирус:

  - В исключения антивируса должны быть добавлены правила, которые разрешают доступ к основному узлу PT Sandbox и используемым прокси-серверам по протоколам HTTP и HTTPS.
  - В PT Sandbox должен быть установлен пользовательский SSL-сертификат, выпущенный доверенным центром сертификации.

6. Анонимная проверка объектов

Вы можете анонимно проверять по одному файлу или ссылке через веб-интерфейс PT Sandbox, не выполняя аутентификацию.

Примечание. Анонимная проверка должна быть включена администратором PT Sandbox в основных параметрах системы.

► Чтобы проверить объект:

1. В адресной строке браузера введите адрес веб-интерфейса PT Sandbox.

   Откроется страница анонимной проверки объектов.

2. Выберите тип объекта.
3. Если вы выбрали **Файл**, перетащите файл в область загрузки на странице или загрузите его по ссылке **выберите**.
4. Если вы выбрали **Ссылка**, введите ссылку.
5. Если вы хотите проверить архив, защищенный нестандартным паролем, в поле **Пароли для архива** укажите этот пароль.
6. Нажмите кнопку **Проверить**.

   Откроется карточка задания на проверку объекта.

   Примечание. Вы можете вернуться на страницу анонимной проверки, нажав < .

7. Вход в PT Sandbox

Пользовательский интерфейс PT Sandbox доступен в браузере. Вход зарегистрированного пользователя в PT Sandbox выполняется через сервис управления пользователями и доступом PT Management and Configuration (PT MC), который обеспечивает механизм единого входа (технология single sign-on) в продукты Positive Technologies.

Перед входом в PT Sandbox убедитесь, что администратор PT Sandbox или администратор сервиса PT MC предоставил вам:

— ссылку для доступа к интерфейсу PT Sandbox;

— логин и пароль вашей учетной записи пользователя.

При необходимости обратитесь к администратору PT Sandbox или к администратору сервиса PT MC.

► Чтобы войти в PT Sandbox:

1. В адресной строке браузера введите ссылку, предоставленную вам администратором PT Sandbox или администратором сервиса PT MC.

   Откроется страница входа в PT Sandbox.

   Примечание. Если разрешена анонимная проверка файлов, откроется страница для такой проверки.

2. Нажмите кнопку **Войти**.

   Откроется страница входа в PT MC.

3. Выполните одно из следующих действий:

   - Если вы входите под локальной учетной записью, то на вкладке **Локальный** укажите логин локальной учетной записи.
   - Если вы входите под доменной учетной записью, то на вкладке **LDAP** укажите логин доменной учетной записи.

4. В поле **Пароль** введите пароль вашей учетной записи.

5. Нажмите кнопку **Войти**.

   Откроется страница **Задания** со списком заданий на проверку.

   Примечание. Если вы выполняете первый вход после обновления версии PT Sandbox, откроется страница для принятия лицензионного соглашения.

8. Интерфейс PT Sandbox

Все действия в PT Sandbox вы можете выполнять с помощью графического пользовательского интерфейса. В этом разделе приводится описание основных элементов интерфейса PT Sandbox, доступных после входа в PT Sandbox.

В этом разделе

8.1. Главное меню

В верхней части любой страницы интерфейса PT Sandbox расположено главное меню. Главное меню PT Sandbox является ключевым элементом управления в интерфейсе PT Sandbox и обеспечивает доступ к основным функциям PT Sandbox.

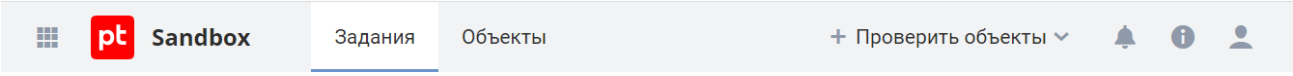

Рисунок 1. Главное меню

В левой части главного меню находится кнопка для перехода в другие приложения Positive Technologies, зарегистрированные в сервисе управления пользователями и доступом PT Management and Configuration (PT MC).

Главное меню содержит разделы для перехода к страницам интерфейса:

— **Задания** — переход к странице со списком заданий на проверку;

— **Объекты** — доступ к хранилищу объектов;

В правой части главного меню расположены:

— Кнопка **Проверить объекты** для выборочной проверки объектов.

— Значок , по нажатию на который открывается Центр уведомлений (см. раздел 8.2).

  На значке отображается количество уведомлений о результатах проверки файлов и ссылок.

— Значок , по нажатию на который вы можете увидеть установленную версию PT Sandbox и версии, доступные для установки, получить информацию о состоянии компонентов PT Sandbox, скачать файлы журналов, перейти на сайт технической поддержки Positive Technologies.

— Значок , по нажатию на который вы можете просмотреть логин, с которым вы вошли в PT Sandbox, сменить тему оформления и язык интерфейса, а также завершить работу под текущей учетной записью.

8.2. Центр уведомлений

По нажатию на значок в главном меню открывается Центр уведомлений. Центр уведомлений — это всплывающее окно, в котором отображаются уведомления о проверке файлов, отправленных вами через интерфейс, а также уведомления об обновлении PT Sandbox.

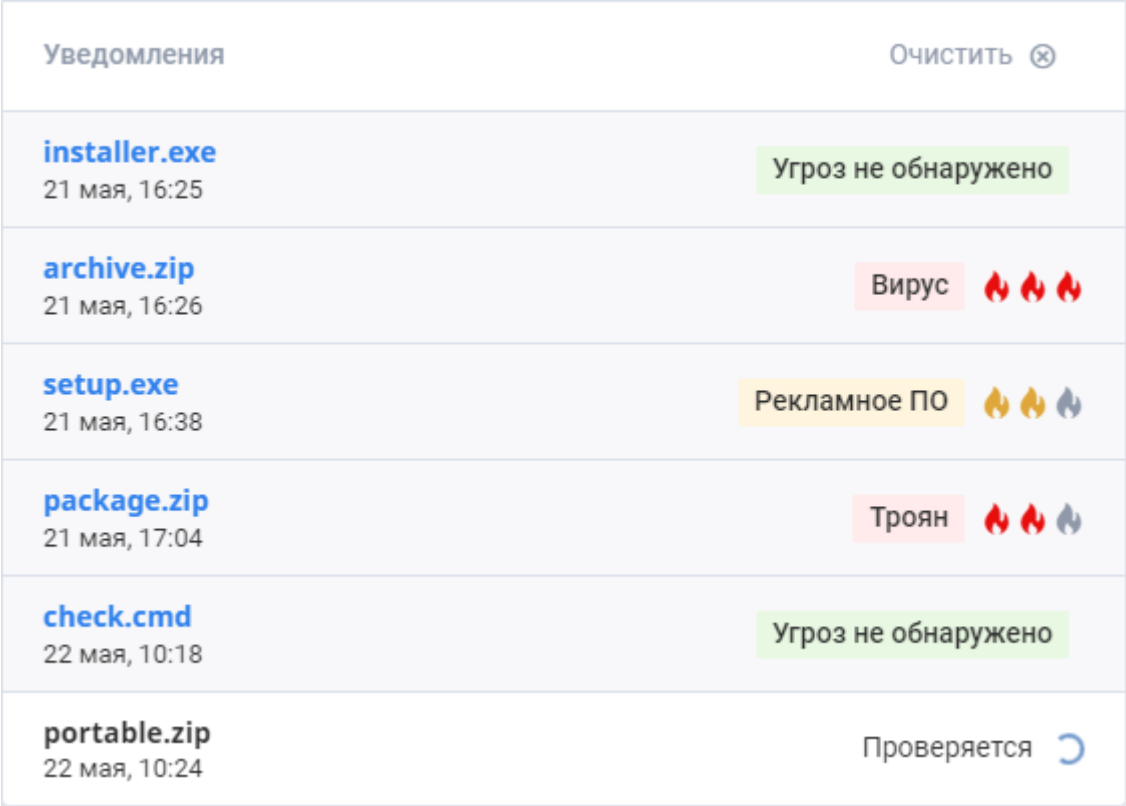

Рисунок 2. Центр уведомлений

В уведомлении о том, что файл проверяется (на белом фоне) отображаются имя файла и время начала проверки. Вы не можете удалять такие уведомления из Центра уведомлений, PT Sandbox удаляет их по завершении проверки.

В уведомлении о результате проверки файла отображаются название файла, информация о результате проверки файла и время завершения проверки. По нажатию на название файла в уведомлении открывается страница выполненного задания на проверку файла. Вы можете самостоятельно удалить уведомление по кнопке ⊗, которая появляется при наведении курсора мыши. Вы также можете удалить все уведомления по кнопке **Очистить**.

8.3. Страница «Задания»

При выборе в главном меню раздела **Задания** открывается страница со списком заданий на проверку объектов.

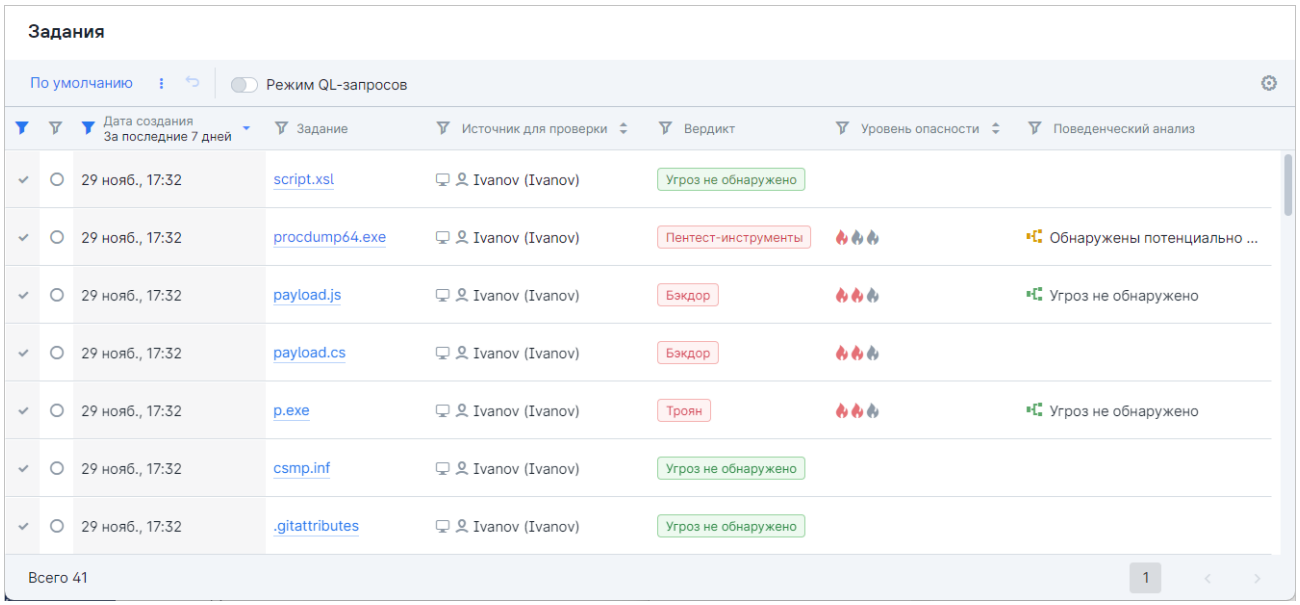

Рисунок 3. Список заданий на проверку

В панели инструментов страницы расположены:

— Кнопка **<Название фильтра>** для выбора фильтра. По кнопке раскрывается меню, в котором вы можете выбрать один из сохраненных фильтров или фильтр по умолчанию. В верхней части меню доступно поле для быстрого поиска фильтра.

— Кнопка ⋮ для выбора дополнительных действий с фильтром. После настройки параметров фильтрации по этой кнопке вы можете сохранить их как новый фильтр или сбросить все изменения. После изменения параметров созданного ранее фильтра по этой кнопке вы можете сохранить для него измененные параметры фильтрации, сохранить параметры фильтрации как новый фильтр, сбросить все изменения, переименовать фильтр или удалить его.

— Кнопка ↩ для выбора фильтра по умолчанию.

— Переключатель **Режим QL-запросов** для создания фильтра с помощью языка запросов QL. В этом режиме появляется поле для ввода QL-запросов, кнопки < и > для выбора предыдущего или следующего запроса и кнопка для просмотра списка выполненных ранее запросов.

— Кнопка для выбора столбцов таблицы.

В рабочей области страницы расположена таблица со списком заданий на проверку. По ссылке в строке задания вы можете открыть карточку задания. В зависимости от вашего выбора, таблица может содержать следующие столбцы с информацией о задании:

— **Статус проверки** — в столбце отображается значок статуса проверки задания:

— проверка не выполнена;

— проверка выполнена частично;

— проверка завершена;

— выполняется проверка.

— **Действие** — в столбце отображается значок, показывающий, был ли файл пропущен в информационную систему организации:

— заблокировано;

— пропущено;

— действие не совершено.

— **Карантин** — в столбце отображается значок, показывающий, был ли файл помещен в карантин:

— в карантине;

— удалено из карантина;

Отсутствие значка указывает на то, что файл не помещался в карантин.

— **Дата создания** — в столбце указаны дата и время добавления задания. По умолчанию в таблице отображаются задания за последние 7 дней.

— **Задание** — в столбце указано название проверяемого объекта.

— **Источник для проверки** — в столбце указаны имя пользователя, который отправил объект на проверку через веб-интерфейс PT Sandbox, и логин его учетной записи.

— **Вердикт** — в столбце указан вердикт по заданию и, если обнаружены объекты с вредоносным ПО, тип обнаруженного ПО.

— **Уровень опасности** — в столбце отображается значок, показывающий уровень опасности обнаруженного вредоносного ПО. Выделяются три уровня для опасного ПО — и три уровня для потенциально опасного ПО — .

— **Поведенческий анализ** — в столбце отображается значок, показывающий результат поведенческого анализа:

— обнаружены опасные файлы;

— обнаружены потенциально опасные файлы;

— поведенческий анализ выполнен частично или с ошибками;

— угроз не обнаружено;

Отсутствие значка указывает на то, что поведенческий анализ не проводился.

— **Откуда > Куда** — в столбце указан логин учетной записи пользователя, который отправил объект на проверку через веб-интерфейс PT Sandbox.

8.4. Страница «Объекты»

При выборе в главном меню раздела **Объекты** открывается страница со списком объектов заданий.

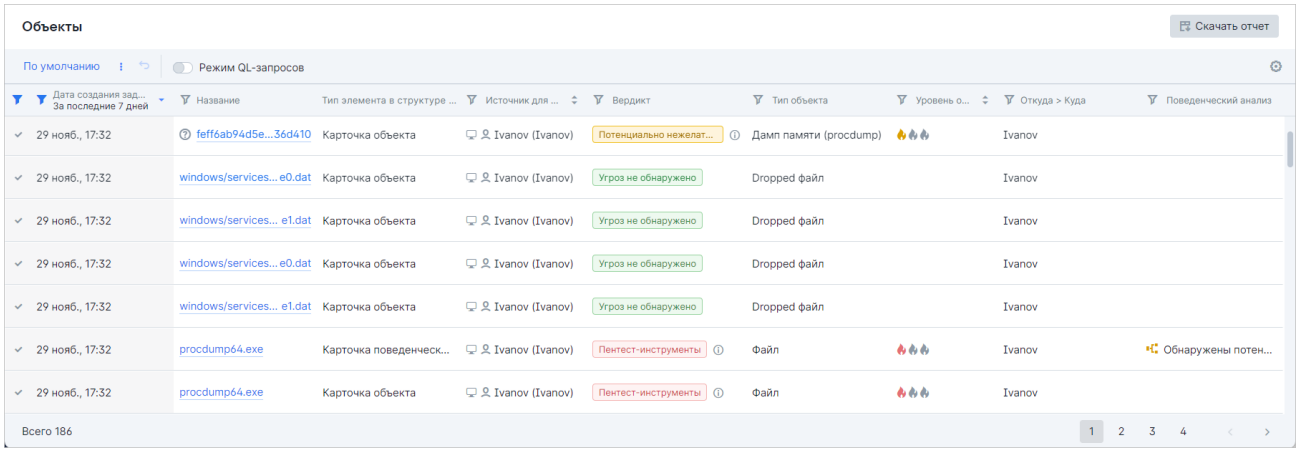

Рисунок 4. Список проверенных объектов

Вверху страницы расположена кнопка **Скачать отчет** для сохранения списка проверенных объектов в файле формата CSV.

В панели инструментов страницы расположены:

— Кнопка **<Название фильтра>** для выбора фильтра. По кнопке раскрывается меню, в котором вы можете выбрать один из сохраненных фильтров или фильтр по умолчанию. В верхней части меню доступно поле для быстрого поиска фильтра.

— Кнопка ⋮ для выбора дополнительных действий с фильтром. После настройки параметров фильтрации по этой кнопке вы можете сохранить их как новый фильтр или сбросить все изменения. После изменения параметров созданного ранее фильтра по этой кнопке вы можете сохранить для него измененные параметры фильтрации, сохранить параметры фильтрации как новый фильтр, сбросить все изменения, переименовать фильтр или удалить его.

— Кнопка ↩ для выбора фильтра по умолчанию.

— Переключатель **Режим QL-запросов** для создания фильтра с помощью языка запросов QL. В этом режиме появляется поле для ввода QL-запросов, кнопки < и > для выбора предыдущего или следующего запроса и кнопка 🕘 для просмотра списка выполненных ранее запросов.

— Кнопка ⚙ для выбора столбцов таблицы.

В рабочей области страницы расположена таблица со списком проверенных объектов. По ссылке в строке объекта вы можете открыть карточку объекта. В зависимости от вашего выбора таблица может содержать следующие столбцы с информацией об объектах:

— **Статус проверки** — в столбце отображается значок статуса проверки объекта:

■ — проверка не выполнена;

◪ — проверка выполнена частично;

✓ — проверка завершена;

— выполняется проверка.

- **Дата создания задания** — в столбце указаны дата и время добавления задания на проверку объекта. По умолчанию в таблице отображаются объекты заданий, созданных за последние 7 дней.
- **Название** — в столбце указано название объекта, с которым он впервые поступил на проверку.
- **Тип элемента в структуре задания** — в столбце указано, является ли этот элемент карточкой объекта или карточкой поведенческого анализа.
- **Источник для проверки** — в столбце указаны имя пользователя, который отправил объект на проверку через веб-интерфейс PT Sandbox, и логин его учетной записи.
- **Вердикт** — в столбце указан вердикт по объекту. Если в объекте обнаружено вредоносное ПО, указан его тип. По кнопке ⓘ вы можете посмотреть, какими средствами проверки вредоносное ПО было обнаружено.
- **Тип объекта** — в столбце указан тип объекта.
- **Уровень опасности** — в столбце отображается значок, показывающий уровень опасности обнаруженного вредоносного ПО. Выделяются три уровня для опасного ПО — и три уровня для потенциально опасного ПО — .
- **Откуда > Куда** — в столбце указан логин учетной записи пользователя, который отправил объект на проверку через веб-интерфейс PT Sandbox.
- **Поведенческий анализ** — в столбце отображается значок, показывающий результат поведенческого анализа:

  — обнаружены опасные файлы;

  — обнаружены потенциально опасные файлы;

  — поведенческий анализ выполнен частично или с ошибками;

  — угроз не обнаружено;

  Отсутствие значка указывает на то, что поведенческий анализ не проводился.
- **Идентификатор задания** — в столбце указан идентификатор задания, по которому проверен объект.
- **Объект получен** — в столбце указано, откуда получен объект:
  - **От источника** — объект поступил на проверку от источника.
  - **Из архива** — файл получен в результате распаковки архива.
  - **Из письма** — файл является телом или вложением письма.
  - **Из тела письма** — ссылка извлечена из тела письма.
  - **Из файла** — ссылка извлечена из файла, тела письма или вложения.

- **По ссылке** — файл скачан по ссылке.
- **Из HTTP-сообщения** — файл получен в результате HTTP-запроса.
- **В результате ПА** — объект является артефактом поведенческого анализа.

— **Причина вердикта** — для объектов с угрозами в столбце указаны средства проверки, которыми эта угроза была обнаружена. Если указано **Наследуемый вердикт**, то причиной вердикта стал результат проверки дочерних объектов.

— **MIME-тип** — в столбце указан формат файла, записанный в виде MIME-типа (см. приложение А).

— **SHA-256**, **SHA-1**, **MD5** — в столбцах указана хеш-сумма файла в различных форматах.

— **Метки** — в столбце указаны особенности объекта.

— **Черный и белый списки** — в столбце указано, находился ли файл в черном или белом списке на момент проверки:

В черном списке;

В белом списке;

Если ничего не указано, то файл на момент проверки отсутствовал в списках.

— **Название образа ВМ** — в столбце указано название образа ВМ, на котором выполнялся поведенческий анализ файла.

— **Продолжительность анализа** — в столбце указано время выполнения поведенческого анализа файла в минутах.

— **Поведенческий анализ (результат проверки)** — в столбце указан тип вредоносного ПО, обнаруженного при поведенческом анализе..

— **Поведенческий анализ (обнаруженное ВПО)** — в столбце указано название вредоносного ПО, обнаруженного при поведенческом анализе.

— **Потенциально опасное поведение** — в столбце указана информация о подозрительном поведении файла, обнаруженном при поведенческом анализе.

— **Анализ с перезагрузкой ОС** — в столбце указан режим поведенческого анализа файла.

— **Родительский процесс** — в столбце указано название родительского процесса, связанного с вредоносным ПО, которое было обнаружено при поведенческом анализе.

— **<Средство проверки> (результат проверки)** — в столбце указан тип вредоносного ПО, обнаруженного этим средством проверки.

— **<Средство проверки> (обнаруженное ВПО)** — в столбце указано название вредоносного ПО, обнаруженного этим средством проверки.

8.5. Карточка задания и карточки объектов

Страница карточки задания открывается по нажатию на строку таблицы на странице **Задания**. Карточка задания содержит карточки отдельных объектов, проверенных в ходе выполнения этого задания. Страница карточки объекта открывается из карточки задания или по нажатию на строку таблицы на странице **Объекты**.

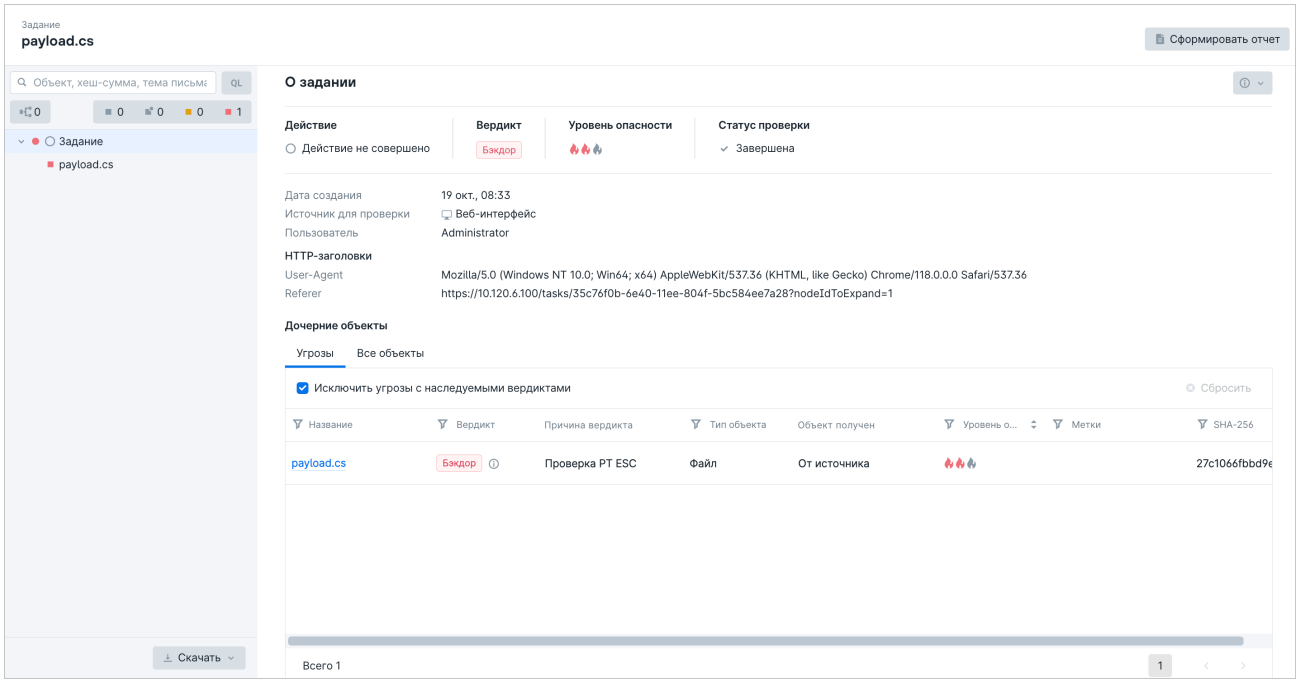

Рисунок 5. Карточка задания

В верхней части страницы с карточкой задания или карточкой объекта указывается название задания и находится кнопка **Сформировать отчет** для выпуска отчета по заданию (см. раздел 12.3). В левой части страницы расположена панель для выбора объектов задания. В панели расположены:

— Блок поиска и фильтрации. В этом блоке вы можете искать объекты через обычный поиск или с помощью языка запросов (см. приложение Б). Здесь вы также можете отфильтровать объекты, используя следующие кнопки:

  - Показать только объекты поведенческого анализа;
  - Показать непроверенные объекты;
  - Показать частично проверенные объекты;
  - Показать потенциально опасные объекты;
  - Показать опасные объекты.

— Иерархический список файлов задания и объектов поведенческого анализа.

— Кнопка **Скачать**, которая позволяет скачать из хранилища файлы, связанные с заданием на проверку (см. раздел 12.4).

Наполнение рабочей области зависит от элемента, выбранного в списке.

Задание

При выборе в иерархическом списке задания в рабочей области отображаются:

— Кнопка ⓘ с раскрывающимся списком для скачивания диагностической информации для анализа ложных срабатываний.

— Результат проверки задания: действие, вердикт по всему заданию, который выносится на основании вердиктов по каждому объекту задания, присвоенный уровень опасности и статус проверки.

— Общая информация о задании: дата создания задания, источник, с которого была инициирована проверка, пользователь, который запустил проверку.

— Дополнительная информация по источнику для проверки:

- HTTP-заголовки (при проверке через веб-интерфейс PT Sandbox);
- SMTP-адреса (при проверке через почтовые источники).

— Таблица с дочерними объектами. Вы можете отфильтровать объекты в таблице, а также посмотреть информацию о вердикте, нажав ⓘ. В таблице отображаются:

- все объекты с угрозами на вкладке **Угрозы**. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.
- все объекты задания на вкладке **Все объекты**. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.

При выборе задания, содержащего письмо от почтовых источников «Почтовый сервер с установленным агентом» и «Почтовый сервер в режиме фильтрации» в рабочей области задания также отображается ссылка **Показать детали доставки**, по которой открывается боковая панель с информацией о доставке письма SMTP-сервером.

Файл

При выборе файла в иерархическом списке в рабочей области отображаются:

— Кнопка **Перепроверить** для повторной проверки файла.

— Кнопка ⓘ с раскрывающимся списком для скачивания диагностической информации для анализа ложных срабатываний.

— Свойства файла.

— Ссылка **Найти этот объект в других заданиях**, по которой открывается новая вкладка браузера с разделом **Объекты** главного меню — списком заданий, в которых проверялся объект.

— Ссылка **Проверить объект по базе VirusTotal**, по которой открывается новая вкладка с результатами проверки объекта в сторонней базе.

— Вердикт по файлу и статус проверки.

— Информация о том, находились ли хеш-суммы файла в черном или белом списке на момент проверки. Нажав на ссылку **Найти файл в списках**, вы можете обновить информацию о нахождении файла в списках, а также добавить его в черный или белый список.

— Результаты статического и поведенческого анализа файла.

— Результаты проверки в соответствии с дополнительными критериями определения потенциально опасных файлов.

— Таблица с дочерними объектами. Вы можете отфильтровать объекты в таблице, а также посмотреть информацию о вердикте, нажав ⓘ. В таблице отображаются:

- все объекты с угрозами на вкладке **Угрозы**. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.
- все объекты задания на вкладке **Все объекты**. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.

Письмо

При выборе в иерархическом списке письма в рабочей области отображаются:

— Кнопка **Перепроверить** для повторной проверки письма и всех его вложений.

— Свойства письма.

— Тема и текст сообщения письма. Для текста сообщения письма отображаются ссылки **Показать** и **Скрыть**, которые позволяют управлять отображением содержимого, и ссылка **HTML-версия**, по которой сообщение письма открывается в HTML-формате (при наличии).

— Ссылка **Найти этот объект в других заданиях**, по которой открывается новая вкладка браузера с разделом **Объекты** главного меню—списком заданий, в которых проверялся объект.

— Ссылка **Проверить объект по базе VirusTotal**, по которой открывается новая вкладка с результатами проверки объекта в сторонней базе.

— Вердикт по файлу и статус проверки.

— Результат статического анализа файла.

— Информация о том, находились ли хеш-суммы файла письма в черном или белом списке на момент проверки. Нажав на ссылку **Найти файл в списках**, вы можете обновить информацию о нахождении файла письма в списках, а также добавить его в черный или белый список.

— Результаты проверки в соответствии с дополнительными критериями определения потенциально опасных файлов.

— Таблица с дочерними объектами. Вы можете отфильтровать объекты в таблице, а также посмотреть информацию о вердикте, нажав ⓘ. В таблице отображаются:

- все объекты с угрозами на вкладке **Угрозы**. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.
- все объекты задания на вкладке **Все объекты**. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.

Ссылка

При выборе в иерархическом списке ссылки в рабочей области отображаются:

— Кнопка **Перепроверить** для повторной проверки ссылки.

— Кнопка **Скопировать** для копирования ссылки — объекта проверки.

— Свойства ссылки: исходная ссылка и средство проверки, с помощью которого она была обработана.

— Ссылка **Найти этот объект в других заданиях**, по которой открывается новая вкладка браузера с разделом **Объекты** главного меню — списком заданий, в которых проверялся объект.

— Вердикт по ссылке и статус проверки.

— Таблица с дочерними объектами. Вы можете отфильтровать объекты в таблице, а также посмотреть информацию о вердикте, нажав ⓘ. В таблице отображаются:

- все объекты с угрозами на вкладке **Угрозы**. Если требуется, вы можете отключить отображение угроз с наследуемыми вердиктами, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.
- все объекты задания на вкладке **Все объекты**. Если требуется, вы можете включить отображение только дочерних объектов первого уровня, установив соответствующий флажок. При нажатии на название объекта открывается его карточка, в которой вы можете посмотреть информацию о проверке объекта.

См. также

Страница «Задания» (см. раздел 8.3)

Страница «Объекты» (см. раздел 8.4)

8.6. Карточка поведенческого анализа

В карточке собрана вся информация и артефакты, которые были сформированы в ходе поведенческого анализа. В карточке вы можете найти и отфильтровать объекты поведенческого анализа, посмотреть диаграмму поведения файла и узнать результат поведенческого анализа. Открыть карточку поведенческого анализа можно через раздел **Объекты** главного меню, выбрав в столбце **Тип элемента в структуре задания** значение **Карточка поведенческого анализа**, или через раздел **Задания**, выбрав задание, для которого был проведен поведенческий анализ.

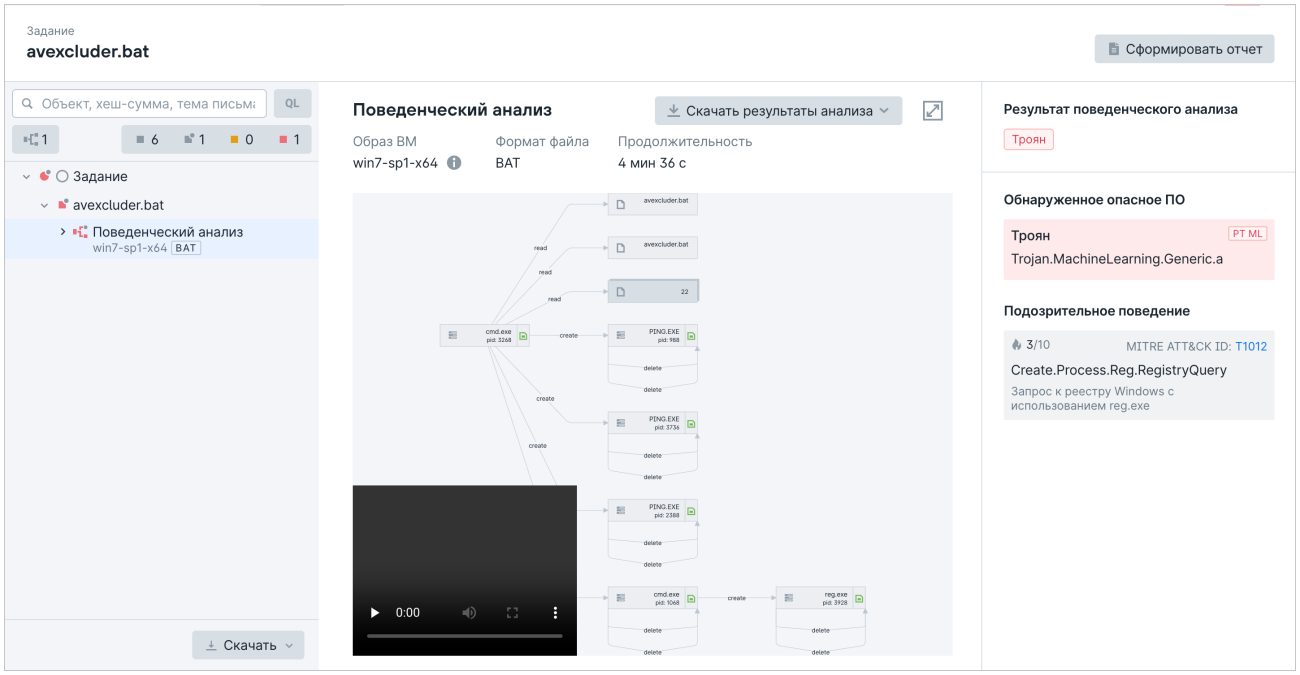

Рисунок 6. Карточка поведенческого анализа

Вверху страницы справа отображается кнопка **Сформировать отчет**, нажав которую можно создать отчет по проверенным объектам (см. раздел 12.5). Рабочая область карточки разделена на три панели.

В панели слева вы можете выбрать объекты поведенческого анализа. Эта панель состоит из следующих элементов:

— Блок поиска и фильтрации. В этом блоке вы можете искать объекты через обычный поиск или с помощью языка запросов (см. приложение Б). Здесь вы также можете отфильтровать объекты, используя следующие кнопки:

  - Показать только объекты поведенческого анализа;
  - Показать непроверенные объекты;
  - Показать частично проверенные объекты;
  - Показать потенциально опасные объекты;
  - Показать опасные объекты.

— Иерархический список файлов задания и объектов поведенческого анализа.

— Кнопка **Скачать**, которая позволяет скачать из хранилища файлы, связанные с заданием на проверку (см. раздел 12.4).

В центральной панели отображается информация об образе ВМ, формате файла, продолжительности наблюдения за файлом. В панели также расположены следующие элементы:

— Кнопка **Скачать результаты анализа**, нажав которую, вы можете выбрать, какие файлы нужно скачать (см. раздел 12.2.4).

— Диаграмма поведения файла. На диаграмме поведения файла отображаются объекты, которые обозначены прямоугольниками, и стрелки, которые показывают связи между объектами: создание, изменение, чтение данных или удаление. При нажатии на прямоугольник в правой панели страницы отображается информация об объекте. На диаграмме могут отображаться следующие типы объектов:

  — процесс (если для процесса проверялся дамп памяти, то для объекта также отображается значок);

  — файл или группа файлов;

  — обращение к реестру или группе реестров;

  — служба;

  IP — IP;

  — сокет;

  URL —сервер или гиперссылка;

  — сетевой пакет;

  — мьютекс;

  — именованный канал;

  —точка соединения, жесткая ссылка или символическая ссылка.

— Окно для просмотра видеозаписи поведения файла в ОС, если при проверке объекта не была отключена запись видео (см. раздел 9.1).

Примечание. Вы можете увеличить масштаб диаграммы двойным щелчком мыши и управлять масштабом диаграммы колесом мыши. По нажатию кнопки вы можете расширить область диаграммы для удобства просмотра. При этом левая и правая панели страницы будут скрыты. Вы можете восстановить их, повторно нажав кнопку .

В правой панели страницы вы можете просмотреть информацию о выбранном объекте диаграммы. Если объект на диаграмме не выбран, то отображается информация о результате поведенческого анализа, которая разделена на следующие блоки:

— Блок **Результат поведенческого анализа**. В этом блоке отображается конечный результат поведенческого анализа — тип обнаруженной угрозы.

— Блок **Обнаруженное опасное ПО**. Блок отображается, если в ходе поведенческого анализа было обнаружено такое ПО. В карточке по каждому опасному ПО отображается его название и метод, с помощью которого оно было обнаружено при проверке.

  Примечание. Вы можете скопировать название обнаруженного вредоносного ПО, нажав кнопку .

— Блок **Подозрительное поведение**. В этом блоке по каждому обнаруженному подозрительному поведению отображается его описание, уровень опасности и идентификатор техники MITRE ATT&CK, при нажатии на который открывается страница с информацией о технике на сайте MITRE ATT&CK.

8.7. Смена языка и темы оформления интерфейса

Интерфейс PT Sandbox доступен на русском и английском языках в светлой и темной темах оформления. По умолчанию выбраны русский язык и светлая тема.

► Чтобы сменить язык интерфейса,

  в главном меню нажмите , в раскрывшемся меню выберите пункт **Язык** и название языка.

  Язык интерфейса изменен.

► Чтобы сменить тему интерфейса,

  в главном меню нажмите , в раскрывшемся меню выберите пункт **Тема** и название темы.

  Примечание. Для выбора темы, соответствующей оформлению интерфейса ОС, вы можете выбрать **Системная**.

  Тема интерфейса изменена.

9. Проверка объектов

Через интерфейс PT Sandbox вы можете отправлять на проверку файлы и ссылки на файлы. Кроме того, если в PT Sandbox настроена служба Checkme, вы можете отправлять на проверку файлы и письма по электронной почте.

Внимание! Максимальный размер файла, который вы можете отправить на проверку через интерфейс PT Sandbox, — 1 ГБ.

В этом разделе

9.1. Параметры проверки объектов

При проверке объектов через интерфейс вы можете настроить параметры проверки.

Поведенческий анализ

При включении параметра вы сможете настроить поведенческий анализ файлов. Такой анализ выполняется только для некоторых типов файлов (см. приложение А). Проверяемый файл запускается на виртуальной машине, развернутой из определенного образа, и отслеживается его поведение.

По кнопке **Добавить образ** вы можете добавить несколько образов ВМ. Добавляйте образы только с теми ОС, которые используются в вашей организации. Для каждого образа доступны следующие параметры настройки поведенческого анализа файлов:

- **Режим с перезагрузкой ОС** — при включении этого режима PT Sandbox отслеживает поведение файлов в ОС до ее перезагрузки и после. Это позволяет обнаружить вредоносное ПО, добавляющее себя в автозагрузку и проявляющее активность только при загрузке ОС.

  Примечание. Режим с перезагрузкой ОС работает только на виртуальных машинах с операционными системами Windows 7 64-разрядной версии и Windows 10.

- **Образ виртуальной машины** — раскрывающийся список для выбора образа ВМ.
- **Типы проверяемых файлов** — раскрывающийся список для выбора типов и форматов проверяемых файлов (список доступен после выбора образов ВМ). Если типы загруженных на проверку файлов отличаются от тех, что указаны для образов, то такие файлы не будут проверяться методом поведенческого анализа.

— **Продолжительность наблюдения за файлом** — поля для ввода максимального времени анализа поведения файла в ОС в минутах и секундах. При проверке архивов это время анализа каждого файла из архива. При указании этого параметра учитывайте объем и скорость потока в сочетании с производительностью аппаратных ресурсов.

  Примечание. Для расчета продолжительности наблюдения за файлом вы можете использовать следующие рекомендации: если файлы приложений проверяются N минут, то презентации, таблицы и документы будут проверяться 1 + N/2 минут, а файлы PDF — 0,5 + N/3 минут. Например, если для файлов приложений установлена продолжительность наблюдения 4 минуты, то для презентаций, таблиц и документов это время должно быть 3 минуты, а для файлов PDF — примерно 2 минуты.

— **Расшифровывать и анализировать HTTPS-трафик** — при установленном флажке для расшифровки и анализа защищенного трафика сертификаты ПО подменяются собственным сертификатом PT Sandbox. Если требуется выявить вредоносное ПО, которое проверяет свойства сертификата и перестает работать, обнаружив его подмену, вы можете снять флажок.

— **Отключить запись видео** — установка флажка позволяет отключить запись видео поведения файлов в ОС. При снятии флажка видео записывается, но при этом увеличивается нагрузка на систему.

— **Использовать результаты предыдущих проверок** — при установленном флажке используются результаты предыдущих проверок файлов методом поведенческого анализа. Результат анализа каждого файла хранится в оперативной памяти сервера PT Sandbox в течение 48 часов. Если в течение этого времени такой же файл повторно поступает на поведенческий анализ в том же образе ВМ с такими же настройками, повторный анализ файла не проводится, в этом случае используется результат предыдущей проверки. При снятии флажка результаты предыдущих проверок не используются, но при этом увеличивается нагрузка на систему.

Анализ файлов, найденных в черном или белом списке

В PT Sandbox предусмотрена возможность добавления файлов в черный или белый список. По умолчанию такие файлы не проверяются, файлы из черного списка всегда считаются опасными, из белого списка — безопасными.

Продолжать проверку файла после его обнаружения в одном из списков — флажок для включения проверки файлов, которые уже добавлены в исключения.

Проверка архивов

При проверке архивов, защищенных паролем, PT Sandbox использует список стандартных паролей, который настраивается специалистом по безопасности в главном меню в разделе **Система** на странице **Основные параметры**. В поле **Пароли для архивов** вы можете указать другие пароли для проверки архивов (по одному паролю в каждой строке).

Глубина распаковки архивов — поле для ввода максимального количества вложенных друг в друга архивов, которые будут распаковываться при проверке. Увеличение глубины распаковки архивов снижает скорость проверки. Если распаковывать архивы не требуется, вы можете ввести `0`, тогда архивы будут проверяться как обычные файлы.

Проверка контента по ссылкам

Проверка контента выполняется по добавленным ссылкам и по ссылкам, извлеченным из добавленных файлов. По ссылкам, которые не содержат индикаторов компрометации, скачивается контент и в виде файлов отправляется на проверку. Для извлеченных из файлов ссылок вы можете настроить дополнительные параметры фильтрации:

— **Адреса для проверки контента** — поле для ввода проверяемых адресов. Контент будет скачиваться и проверяться только по ссылкам на указанные адреса. Вы можете указать имена доменов, поддоменов, IP-адреса узлов или адреса подсетей в формате CIDR. Ссылки на IP-адрес и доменное имя одного и того же ресурса считаются разными ссылками. При вводе адресов вы можете использовать звездочку:

- Если необходимо проверять контент по ссылкам на любые адреса, вы можете ввести `*`.

  Внимание! При пустом поле контент будет проверяться только по тем ссылкам, которые система определит как подозрительные.

- Если необходимо проверять контент по ссылкам на определенный домен, вы можете ввести `*<Имя домена>`, например `*example.com`.

- Если необходимо проверять контент по ссылкам на любые поддомены одного домена, вы можете ввести `*.<Имя домена>`, например `*.example.com`.

— **Исключаемые адреса** — поле для ввода исключаемых адресов. По ссылкам на эти адреса контент скачиваться не будет. Вы можете указать имена доменов, поддоменов, IP-адреса узлов или адреса подсетей в формате CIDR. При вводе адресов вы можете использовать звездочку. Приоритет исключаемых адресов выше приоритета адресов для проверки.

— **Включить эвристику** — при установленном флажке контент будет проверяться по ссылкам, которые система определит как подозрительные.

— **Ограничить количество ссылок для скачивания до** — при установленном флажке вы можете указать количество ссылок в задании, по которым будет скачиваться и проверяться контент. При снятом флажке контент будет проверяться по всем извлеченным в задании ссылкам.

Дополнительные критерии определения потенциально опасных файлов

В этом блоке вы можете указать, какие еще объекты, кроме определяемых системой, необходимо относить к потенциально опасным:

— **Архивы** — при установке флажков PT Sandbox относит к потенциально опасным файлы архивов:

  - **Зашифрованные и нераспакованные** — которые не удалось распаковать.

    Примечание. Перечень стандартных паролей, которые используются при распаковке архивов, вы можете указать в основных параметрах системы.

  - **С превышенной глубиной распаковки** — глубина распаковки которых превышает значение, указанное в параметре **Глубина распаковки архивов**.

— **Файлы офисных форматов** — при установке флажков PT Sandbox относит к потенциально опасным файлы офисных приложений Microsoft Office (Word, Excel, PowerPoint) и OpenDocument:

  - **Зашифрованные** — которые защищены паролем.
  - **С макросами** — в которых используются макросы.
  - **С внедренными объектами (OLE)** — в которых есть внедренные объекты.
  - **С элементами ActiveX** — в которых используются элементы ActiveX[1].
  - **С запросами к внешним данным** — в которых есть запросы к внешним ресурсам с данными[1].
  - **Использующие шаблон** — в которых есть ссылки на внешние шаблоны[1].
  - **С функциями DDE** — в которых используются функции динамического обмена данными[1].
  - **С настроенными действиями (Actions)** — в которых настроены автоматические действия[1].

— **Файлы PDF** — при установке флажков PT Sandbox относит к потенциально опасным файлы PDF:

  - **Зашифрованные** — которые защищены паролем.
  - **С внедренными объектами (OLE)** — в которых есть внедренные объекты.
  - **С настроенными действиями при открытии (OpenActions)** — в которых настроены автоматические действия при открытии.

1 Поддерживается только для файлов Microsoft Office версии 2007 или выше.

- **С настроенными действиями (Actions)** — в которых настроены другие автоматические действия.
- **Со сценариями JavaScript** — в которых есть сценарии JavaScript.

9.2. Проверка файлов через интерфейс

► Чтобы проверить файлы через интерфейс PT Sandbox:

1. В главном меню нажмите кнопку **Проверить объекты**.

   Откроется окно **Проверка объектов**.

2. На вкладке **Файлы** перетащите файлы для проверки в область загрузки или нажмите на ссылку **выберите**.

   В окне появится информация о загруженных файлах.

   Примечание. Вы можете отменить отправку файла на проверку по кнопке ⊗ и добавить другие файлы, перетащив их в область загрузки файлов или по ссылке **выберите**.

3. Настройте параметры проверки файлов (см. раздел 9.1).
4. Нажмите кнопку **Проверить**.

Файлы отправлены на проверку, для каждого файла создано отдельное задание на проверку. В Центре уведомлений появились уведомления о статусе выполнения этих заданий.

9.3. Проверка ссылок через интерфейс

► Чтобы проверить ссылку:

1. В главном меню нажмите кнопку **Проверить объекты**.

   Откроется окно **Проверка объектов**.

2. На вкладке **Ссылки** укажите в поле одну или несколько ссылок.

   Примечание. Если по ссылке находится файл, размер которого превышает 1 ГБ, PT Sandbox скачивает первый гигабайт файла и проверяет его.

3. Если требуется, настройте параметры проверки (см. раздел 9.1).
4. Нажмите кнопку **Проверить**.

Ссылки отправлены на проверку, для каждой ссылки создано отдельное задание на проверку. В Центре уведомлений появились уведомления о статусе выполнения этих заданий.

9.4. Проверка ссылок из карточки задания

Задания на проверку писем могут содержать ссылки, извлеченные из тела письма или из вложенного в письмо файла. Часть из этих ссылок может быть не проверена автоматически. Вы можете запустить проверку таких ссылок вручную.

► Чтобы запустить проверку ссылки из карточки задания:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Щелчком мыши по строке в таблице откройте карточку задания.
3. В иерархическом списке выберите **Тело письма** или название вложенного файла.
4. В раскрывающемся блоке **Извлеченные ссылки, для которых не выполнялась проверка контента** нажмите ⌄.
5. В строке со ссылкой нажмите **Проверить**.

   Откроется окно для настройки параметров проверки.

6. Если требуется, настройте параметры проверки (см. раздел 9.1).
7. Нажмите кнопку **Проверить**.

Ссылка отправлена на проверку, создано задание на проверку. В Центре уведомлений появилось уведомление о статусе выполнения этого задания.

9.5. Отправка файлов на проверку по электронной почте

Вы можете отправлять файлы на проверку по электронной почте и получать результаты проверки в ответных письмах.

Перед отправкой файлов на проверку вам нужно получить от администратора PT Sandbox адрес электронной почты, предназначенный для проверки файлов.

► Чтобы проверить файлы по электронной почте:

1. В вашей почтовой программе откройте форму создания письма.
2. В поле получателя введите адрес электронной почты для проверки файлов.

   Внимание! Не добавляйте других адресатов, иначе письмо не будет доставлено в PT Sandbox.

3. Если предназначенные для проверки файлы запакованы в архивы и защищены известными вам паролями, в тексте письма введите по одному уникальному паролю в каждой строке.

Примечание. Если вы не знаете пароль к архиву, PT Sandbox попытается распаковать архив, используя список стандартных паролей, который задается специалистом по безопасности PT Sandbox.

4. Прикрепите к письму файлы, которые вам нужно проверить.

   Примечание. Вы можете уточнить максимально допустимый размер почтового вложения у администратора PT Sandbox.

5. Отправьте письмо.

   PT Sandbox проверит как текст письма, так и его вложения. По окончании проверки PT Sandbox отправит вам ответное письмо с ее результатами.

6. В полученном письме нажмите кнопку **Отчет о сканировании**, чтобы просмотреть в интерфейсе PT Sandbox результаты проверки отправленного вами письма с вложениями.

10. Поиск результатов проверки

Вы можете искать результаты проверки файлов, отправленных вами на проверку через интерфейс с предварительным входом в PT Sandbox.

В этом разделе приводятся инструкции по поиску заданий с результатами проверки файлов и электронных писем. Вы можете совмещать критерии поиска.

В этом разделе

10.1. Выбор столбцов для отображения на странице заданий

Вы можете управлять отображением столбцов в таблице на странице заданий.

► Чтобы выбрать столбцы для отображения в таблице:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Нажмите ⚙.

3. В открывшемся окне установите флажки напротив названий столбцов, которые нужно отображать в таблице.

   Примечание. Вы можете выбрать набор столбцов по умолчанию, нажав кнопку **Сбросить**.

Выбранные столбцы отобразятся в таблице.

10.2. Поиск заданий по времени создания

► Чтобы найти задания по времени создания:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. В таблице нажмите на заголовок столбца **Дата создания**.
3. Во всплывающем окне выберите предустановленный период или настройте свой.
4. Нажмите кнопку **Применить**.

   PT Sandbox отобразит в списке только те задания, которые были созданы за выбранный вами период.

10.3. Поиск заданий по вердикту

► Чтобы найти задания по вердиктам:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.
3. В таблице нажмите на заголовок столбца **Вердикт** и во всплывающем окне установите флажки напротив нужных вам вердиктов.

   Примечание. В этом всплывающем окне вы можете искать типы угроз с помощью поля поиска.

В таблице появятся задания с выбранными вами вердиктами.

10.4. Поиск заданий по состоянию

► Чтобы найти задания по состоянию:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.
3. В первом столбце таблицы нажмите .
4. Во всплывающем окне установите флажки напротив нужных вам состояний.

   PT Sandbox отобразит в списке задания с выбранными вами состояниями.

10.5. Поиск заданий по уровню опасности файлов

Вы можете искать задания по уровню опасности проверенных файлов.

► Чтобы найти задания по уровню опасности файлов:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В таблице нажмите на заголовок **Уровень опасности** и во всплывающем окне установите флажки напротив нужных вам уровней.

   PT Sandbox отобразит в списке задания с выбранными вами уровнями опасности файлов.

10.6. Поиск заданий по источникам для проверки

Вы можете искать задания по источникам, с которых файлы поступали в PT Sandbox.

► Чтобы найти задания по источникам для проверки:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В таблице нажмите на заголовок **Источники для проверки** и во всплывающем окне установите флажки напротив нужных вам источников.

   PT Sandbox отобразит в списке только те задания, которые поступили с выбранных вами источников.

10.7. Поиск заданий по отправителям файлов

Вы можете искать задания по пользователям, которые отправляли файлы на проверку в PT Sandbox через его интерфейс.

► Чтобы найти задания по отправителям файлов:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. Если столбец **Откуда > Куда** не отображается в таблице, настройте его отображение (см. раздел 10.1).
4. В таблице нажмите на заголовок столбца **Откуда > Куда** и в появившемся поле поиска введите логин нужного пользователя.

   PT Sandbox отобразит в списке задания на проверку файлов, которые были отправлены пользователем с указанным логином.

10.8. Поиск заданий по результатам поведенческого анализа

Вы можете искать задания по результатам поведенческого анализа файлов.

► Чтобы найти задания по результатам поведенческого анализа:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.
2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.
3. В таблице нажмите на заголовок столбца **Поведенческий анализ** и во всплывающем окне установите флажки напротив нужных вам результатов поведенческого анализа.

   PT Sandbox отобразит в списке задания с выбранными вами результатами поведенческого анализа.

10.9. Создание фильтра для поиска заданий

Для поиска заданий вы можете создавать фильтры с набором параметров.

Примечание. Созданные вами фильтры недоступны для других пользователей PT Sandbox.

► Чтобы создать фильтр:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.
2. В таблице с заданиями настройте новый фильтр, добавляя или удаляя параметры фильтрации.
3. В панели инструментов страницы нажмите ⋮ и в раскрывшемся меню выберите **Сохранить как новый**.
4. В открывшемся окне в поле **Название** введите название фильтра и нажмите кнопку **Создать**.

Фильтр создан.

10.10. Поиск заданий с помощью языка запросов QL

► Чтобы найти задания с помощью языка запросов QL:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Включите режим ввода QL-запросов.

   На экране появится поле для ввода запроса.

3. Введите запрос, используя синтаксис языка запросов QL.

   Например:

   ```
   age < 30d AND (task.correlated.state != UNKNOWN AND
   task.correlated.verdict.threat.classification IN ("TROJAN")) AND
   task.sandbox.correlated.verdict.threat.level = DANGEROUS
   ```

4. Нажмите клавишу Enter.

На странице **Задания** отобразятся только те задания, которые удовлетворяют введенным критериям поиска.

11. Поиск проверенных объектов

Вы можете искать в хранилище объекты, чтобы просматривать результаты их проверки и скачивать их.

В этом разделе приводятся инструкции по поиску объектов по различным критериям. Вы можете совмещать критерии поиска.

В этом разделе

11.1. Выбор столбцов для отображения на странице объектов

Вы можете управлять отображением столбцов в таблице на странице объектов.

► Чтобы выбрать столбцы для отображения в таблице:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.

2. Нажмите ⚙.

3. В открывшемся окне установите флажки напротив названий столбцов, которые нужно отображать в таблице.

   Примечание. Вы можете выбрать набор столбцов по умолчанию, нажав кнопку **Сбросить**.

Выбранные столбцы отобразятся в таблице.

11.2. Поиск объектов по названиям

► Чтобы найти объект по его названию:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.

2. Если требуется найти объекты, поступившие на проверку за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В таблице нажмите на заголовок столбца **Название**.

4. В появившемся поле поиска введите название или часть названия объекта.

5. Нажмите клавишу Enter.

   PT Sandbox отобразит в списке объекты с указанным вами названием.

11.3. Поиск объектов по времени поступления

► Чтобы найти объекты по времени их поступления в PT Sandbox:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.

2. В таблице нажмите на заголовок столбца **Дата создания**.

3. Во всплывающем окне выберите предустановленный период или настройте свой.

4. Нажмите кнопку **Применить**.

   PT Sandbox отобразит в списке только те объекты, которые поступили в продукт в течение выбранного вами периода.

11.4. Поиск объектов по вердикту

► Чтобы найти объекты по вердиктам:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.

2. Если требуется найти объекты, поступившие на проверку за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В таблице нажмите на заголовок столбца **Вердикт** и во всплывающем окне установите флажки напротив нужных вам вердиктов.

Примечание. В этом всплывающем окне вы можете искать типы угроз с помощью поля поиска.

В таблице появятся объекты с выбранными вами вердиктами.

11.5. Поиск объектов по уровням опасности

► Чтобы найти объекты по уровням опасности:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.

2. Если требуется найти объекты, поступившие на проверку за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В таблице нажмите на заголовок **Уровень опасности** и во всплывающем окне установите флажки напротив нужных вам уровней.

   PT Sandbox отобразит в списке объекты с выбранными вами уровнями опасности.

11.6. Поиск объектов по источникам для проверки

Вы можете искать объекты по источникам, с которых файлы поступали в PT Sandbox.

► Чтобы найти объекты по источникам для проверки:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.

2. Если требуется найти объекты, поступившие на проверку за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В таблице нажмите на заголовок **Источник для проверки** и во всплывающем окне установите флажки напротив нужных вам источников.

   PT Sandbox отобразит в списке только те объекты, которые поступали с выбранных вами источников.

11.7. Поиск объектов по их отправителям

Вы можете искать объекты по пользователям, которые отправляли их на проверку в PT Sandbox через его интерфейс.

► Чтобы найти объекты по отправителям:

1. В главном меню выберите раздел **Объекты**.

Откроется страница **Объекты**.

2. Если требуется найти объекты, поступившие на проверку за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.
3. Если столбец **Откуда > Куда** не отображается в таблице, настройте его отображение.
4. В таблице нажмите на заголовок **Откуда > Куда** и в появившемся поле поиска введите логин нужного пользователя, который отправлял файлы на проверку.

   PT Sandbox отобразит в списке объекты, которые были отправлены пользователем с выбранным вами логином.

11.8. Поиск объектов с помощью языка запросов QL

► Чтобы найти объекты с помощью языка запросов QL:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.
2. Включите режим ввода QL-запросов.

   На экране появится поле для ввода запроса.
3. Введите запрос, используя синтаксис языка запросов QL.

   Например:

   ```
   age < 30d AND (correlated.state != UNKNOW AND correlated.verdict.threat.classification IN
   ("TROJAN"))
   ```
4. Нажмите клавишу Enter.

PT Sandbox отобразит в списке только те объекты, которые удовлетворяют введенным критериям поиска.

11.9. Создание фильтра для поиска объектов

Для поиска объектов вы можете создавать фильтры с набором параметров.

Примечание. Созданные вами фильтры недоступны для других пользователей PT Sandbox.

► Чтобы создать фильтр:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.
2. В таблице со списком объектов настройте новый фильтр, добавляя или удаляя параметры фильтрации.

3. В панели инструментов страницы нажмите ⋮ и в раскрывшемся меню выберите **Сохранить как новый**.
4. В открывшемся окне в поле **Название** введите название фильтра и нажмите кнопку **Создать**.

Фильтр создан.

12. Работа с результатами проверки

После завершения проверки файлов PT Sandbox генерирует отчет с результатами проверки. Если вы отправляли файлы на проверку через интерфейс или по ссылкам, уведомление об окончании проверки со ссылкой на отчет появится в Центре уведомлений. Если вы отправляли файлы на проверку по электронной почте, ссылка на отчет придет в ответном письме.

В этом разделе

12.1. Просмотр результатов проверки

Вы можете просматривать информацию о результатах проверки файлов, отправленных вами в PT Sandbox с помощью его интерфейса или по электронной почте.

► Чтобы просмотреть результат проверки:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания** со списком ваших заданий на проверку.

2. В списке найдите задание, в котором хранится нужный вам результат проверки.

3. Выберите задание в списке.

   Откроется страница, содержащая результат и время проверки файла, название источника, с которого файл поступил на проверку, а также информацию об отправителе файла.

4. В панели слева выберите название проверенного файла.

   Для поиска нужного файла вы можете ввести в поле поиска название файла или использовать фильтры для отображения только опасных, потенциально опасных или непроверенных объектов.

   На странице отобразятся результаты проверки и свойства файла.

   Примечание. Если при проверке зашифрованный архив был распакован с использованием пароля, то этот пароль отображается в свойствах файла.

В случае проверки электронных писем на странице с результатами проверки также отображаются свойства письма.

12.2. Анализ поведения файла в операционной системе

Вы можете анализировать поведение файла в операционной системе и получать информацию об артефактах, которые были созданы этим файлом.

Примечание. Анализ поведения файла возможен только в том случае, если вы отправляли файл на проверку с поведенческим анализом.

В этом разделе приводятся инструкции по работе с результатами поведенческого анализа файлов.

В этом разделе

12.2.1. Просмотр диаграммы поведения файла

Диаграмма поведения файла показывает последовательность действий, которые файл выполняет в операционной системе.

► Чтобы просмотреть диаграмму поведения файла:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В списке заданий выберите задание на проверку, содержащее файл, диаграмму поведения которого вам нужно просмотреть.

   Откроется страница с результатами проверки файлов задания.

   В панели слева отображается список артефактов, которые были созданы проверенным файлом. Для каждого процесса отображается список файлов и дампов памяти. Дампы памяти — это сохраненные фрагменты памяти, которые были изменены наблюдаемым процессом.

4. В панели слева выберите название проверенного файла.

   На странице отобразятся результаты проверки и свойства файла.

5. В панели слева под названием выбранного файла выберите **Поведенческий анализ**.

В рабочей области отобразится диаграмма поведения файла в операционной системе.

6. Если поведенческий анализ выполнялся в режиме с перезагрузкой операционной системы и вам нужно просмотреть диаграмму поведения файла после перезагрузки, выберите соответствующий вариант над диаграммой.

12.2.2. Просмотр списка опасных и потенциально опасных действий файла

► Чтобы просмотреть список опасных и потенциально опасных действий файла:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В списке заданий выберите задание на проверку, содержащее файл, действия которого вам нужно просмотреть.

   Откроется страница с результатами проверки файлов задания.

   В панели слева отображается список артефактов, которые были созданы проверенным файлом. Для каждого процесса отображается список файлов и дампов памяти. Дампы памяти — это сохраненные фрагменты памяти, которые были изменены наблюдаемым процессом.

4. В панели слева выберите название проверенного файла.

   На странице отобразятся результаты проверки и свойства файла.

5. В панели слева под названием выбранного файла выберите **Поведенческий анализ**.

   Список опасных и потенциально опасных действий, которые файл выполнял в операционной системе в ходе поведенческого анализа, отобразится в панели справа в блоке **Поведенческий анализ**.

12.2.3. Просмотр видеозаписи поведения файла

Видеозапись недоступна, если в параметрах проверки файла через веб-интерфейс или в параметрах проверки файлов от источника был установлен флажок **Отключить запись видео**.

► Чтобы просмотреть видеозапись поведения файла:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В списке заданий выберите задание на проверку, содержащее файл, видеозапись поведения которого вам нужно просмотреть.

   Откроется страница с результатами проверки файлов задания.

   В панели слева отображается список артефактов, которые были созданы проверенным файлом. Для каждого процесса отображается список файлов и дампов памяти. Дампы памяти — это сохраненные фрагменты памяти, которые были изменены наблюдаемым процессом.

4. В панели слева выберите название проверенного файла.

   На странице отобразятся результаты проверки и свойства файла.

5. В панели слева под названием выбранного файла выберите **Поведенческий анализ**.

6. В окне проигрывателя нажмите кнопку ▶ .

   Начнется воспроизведение видеозаписи.

   Примечание. Вы можете развернуть окно проигрывателя двойным щелчком мыши по окну или нажав кнопку ⛶, а также перематывать видео при помощи ползунка в нижней части окна.

12.2.4. Скачивание результатов поведенческого анализа

Вы можете загрузить на свой компьютер следующие результаты поведенческого анализа файла:

— журнал событий (`drakvuf-trace.log.gz`) — необработанный список событий в простом текстовом формате;

— нормализованные события (`events-normalized.log.gz`) — события, приведенные к единому виду, пригодному для дальнейшего анализа (в формате JSON);

— скоррелированные события (`events-correlated.log.gz`) — нормализованные события, проанализированные с помощью правил корреляции для нахождения закономерностей и выявления опасного и потенциально опасного поведения (в формате JSON);

— копию трафика (`tcpdump.pcap`) — копию сетевого трафика в формате PCAP.

Вы можете импортировать скачанные файлы в другие программы для самостоятельного анализа или передать для экспертной оценки заинтересованным лицам.

► Чтобы скачать результаты поведенческого анализа:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Если требуется найти задания, созданные за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.

3. В списке заданий выберите задание на проверку файла, результаты поведенческого анализа которого вам нужно скачать.

   Откроется страница с результатами проверки файлов задания.

   В панели слева отображается список артефактов, которые были созданы проверенным файлом. Для каждого процесса отображается список файлов и дампов памяти. Дампы памяти — это сохраненные фрагменты памяти, которые были изменены наблюдаемым процессом.

4. В панели слева выберите название проверенного файла.

   На странице отобразятся результаты проверки и свойства файла.

5. В панели слева под названием выбранного файла выберите **Поведенческий анализ**.

6. Нажмите кнопку **Скачать результаты анализа**.

7. Во всплывающем окне установите флажки напротив нужных вам результатов и нажмите кнопку **Скачать**.

   Примечание. Если файл отправлялся на проверку вручную через веб-интерфейс с включенным режимом с перезагрузкой операционной системы, вы можете выбрать и скачать результаты анализа как до перезагрузки, так и после нее.

   Архив `sandbox_logs.zip` будет загружен на ваш компьютер.

12.2.5. Формат именования типов опасного ПО и подозрительного поведения файлов

Для опасных файлов результат поведенческого анализа отображает информацию о типе обнаруженного опасного ПО. Этот тип может быть определен прямо по поведению файла в виртуальной среде либо по совокупности потенциально опасного поведения. Список потенциально опасных действий, обнаруженных в ходе поведенческого анализа файла, отображается в панели справа. В этой панели есть два блока параметров:

— блок **Обнаруженное опасное ПО**, в котором указывается тип опасного ПО, определенный прямо по поведению файла;

— блок **Подозрительное поведение**, в котором указываются действия, выполняемые файлом в виртуальной среде. По совокупности этих действий может быть сформирован результат поведенческого анализа для блока **Обнаруженное опасное ПО**.

Типы опасного ПО, которые могут отображаться в блоке обнаруженного опасного ПО, имеют формат `<Class>.<Platform>.<Family>.<Modification>`, где:

— `<Class>` — класс вредоносного ПО (примеры возможных значений — `Trojan`, `Backdoor`, `Hacktool`);

— `<Platform>` — платформа или файл, в котором обнаружено вредоносное ПО (примеры возможных значений — `Win32`, `Java`, `VBS`);

— `<Family>` — семейство вредоносного ПО или название инструмента (примеры возможных значений — `HyperBro`, `Kazuar`, `Flame`);

— `<Modification>` — модификация вредоносного ПО (примеры возможных значений — `a`, `b`, `c`).

Потенциально опасные действия файла, которые могут отображаться в блоке потенциально опасного поведения, имеют формат `<Action>.<Object>.<Property>.<Description>`, где:

— `<Action>` — выполняемое действие (примеры возможных значений — `Create`, `Write`, `Delete`);

— `<Object>` — объект, над которым выполняется действие (примеры возможных значений — `Process`, `Registry`, `File`);

— `<Property>` — свойство объекта, на которое направлено действие (примеры возможных значений — `Attribute`, `Data`, `Key`);

— `<Description>` — дополнительная информация об обнаруженном опасном действии файла (примеры возможных значений — `Persistance`, `Evasion`, `UACBypass`).

12.3. Выпуск отчета по заданию

Из карточки задания вы можете сформировать отчет с результатами выполнения задания. В отчет добавляется основная информация о задании и обнаруженных угрозах.

► Чтобы выпустить отчет по заданию:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Щелчком мыши по строке в таблице откройте карточку задания.
3. Нажмите кнопку **Сформировать отчет**.

   Откроется диалоговое окно браузера для настройки печати.

4. Настройте формат выпуска отчета и выпустите его.

В зависимости от выбранного формата выпуска отчет по заданию сохранен на компьютере или отправлен на печать.

12.4. Скачивание файлов задания

► Чтобы скачать из хранилища файлы, связанные с заданием на проверку:

1. В главном меню выберите раздел **Задания**.

   Откроется страница **Задания**.

2. Щелчком мыши по строке в таблице откройте карточку задания.

3. Если требуется скачать все файлы задания, в боковой панели нажмите кнопку **Скачать** и в раскрывшемся меню выберите **Все файлы**.
4. Если требуется скачать отфильтрованные файлы:
   - В боковой панели настройте фильтр файлов.
   - Нажмите кнопку **Скачать** и в раскрывшемся меню выберите **Отфильтрованные**.
5. Если требуется скачать один файл из задания:
   - В боковой панели в иерархическом списке выберите нужный файл.
   - Нажмите кнопку **Скачать** и в раскрывшемся меню выберите **Выбранный файл**.

Связанные с заданием файлы добавлены в ZIP-архив с паролем infected и скачаны на ваш компьютер.

12.5. Создание отчета по объектам

Вы можете создавать отчеты по проверенным объектам. Отчет создается в формате CSV и содержит информацию об объектах, отображаемых на странице.

► Чтобы создать отчет:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.
2. Если требуется найти объекты, поступившие на проверку за определенный период, нажмите в таблице на заголовок столбца **Дата создания** и укажите период.
3. При необходимости найдите в таблице объекты (см. раздел 10), которые нужно отобразить в отчете.
4. Нажмите кнопку **Скачать отчет**.

   Файл отчета будет загружен на ваш компьютер.

12.6. Скачивание проверенных файлов

► Чтобы скачать из хранилища проверенный файл:

1. В главном меню выберите раздел **Объекты**.

   Откроется страница **Объекты**.
2. Щелчком мыши по строке в таблице откройте карточку объекта.
3. Если объект содержит несколько файлов, в боковой панели в иерархическом списке выберите нужный файл.
4. Нажмите кнопку **Скачать** и в раскрывшемся меню выберите **Выбранный файл**.

Примечание. Вы также можете скачать файл, наведя курсор на название файла в боковой панели и нажав ↓.

Файл добавлен в ZIP-архив с паролем infected и скачан на ваш компьютер.

13. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- предоставление рекомендаций по настройке продукта (оптимизации параметров) в процессе его эксплуатации;
- консультации по использованию функциональных возможностей продукта;
- диагностику сбоев, включая поиск причин и информирование клиента о выявленных проблемах;
- предоставление решений или возможностей обойти проблему с сохранением необходимой производительности;
- устранение ошибок в рамках выпуска обновлений;
- рассмотрение предложений по доработке продукта.

Вы можете получать техническую поддержку на специальном портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

13.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

13.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

13.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

13.3.1. Предоставление информации для технической поддержки

Для решения проблем с продуктом вам необходимо предоставить специалисту технической поддержки следующие данные:

— номер лицензии на использование продукта;

— файлы журналов и другие наборы диагностических данных, которые требуются для анализа;

— снимки экрана;

— результаты выполнения рекомендаций специалиста технической поддержки;

— оптимальный канал для удаленного доступа к продукту и его диагностики (выбирается по согласованию).

Если информация не будет предоставлена в течение двух недель с момента запроса, специалист технической поддержки имеет право закрыть заявку, предварительно уведомив вас об этом.

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

13.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

Доработка продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы также можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо доработок. Если Positive Technologies принимает решение о доработке продукта, то способы реализации доработки остаются на усмотрение Positive Technologies.

13.3.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 3).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 3. Время реакции на запрос и время его обработки

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо	До 24 часов	Не ограничено

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
	не оказывающие значительного влияния на бизнес		
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

13.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

Приложение А. Типы файлов, отправляемых на поведенческий анализ

При выполнении поведенческого анализа PT Sandbox проверяет типы файлов, перечисленные в таблице ниже.

Примечание. Некоторые расширения файлов поддерживаются только в образах с определенной ОС.

Таблица 4. Типы файлов, отправляемых на поведенческий анализ

Типы файлов	Подтипы файлов	Расширения файлов
Файлы PDF	—	.pdf
Файлы приложений	Дистрибутивы	.msi, .deb, .rpm
	Исполняемые файлы	.exe, .scr, .elf
	Скрипты	.bat, .cmd, .pl, .ps1, .py, .vbs, .wsf, .sh
	Контейнеры	.chm, .hta
	Пакеты Java	.jar
	Общие библиотеки	.dll
	Ярлыки	.lnk
Презентации	Microsoft PowerPoint 1997—2003	.pot, .ppa, .pps, .ppt
	Microsoft PowerPoint	.potm, .potx, .ppam, .ppsm, .ppsx, .ppt m, .pptx, .sldm, .sldx
	OpenOffice Impress	.odp
Таблицы	Файлы IQY	.iqy
	Microsoft Excel 1997—2003	.xla, .xls, .xlt
	Microsoft Excel	.xlam, .xlsb, .xlsm, .xlsx, .xltm, .xltx
	OpenOffice Calc	.ods, .ots
	Файлы SLK	.slk
Документы	Microsoft Word 1997—2003	.doc, .dot
	Microsoft Word	.docm, docx, .dotm, .dotx
	OpenOffice Writer	.odt, .ott
	Файлы RTF	.rtf

Приложение Б. Синтаксис языка запросов QL

Язык запросов QL используется для поиска объектов через интерфейс PT Sandbox. Операции, поддерживаемые языком запросов, приведены в таблице ниже.

Таблица 5. Поддерживаемые операции

Доступные действия	Пример запроса	Особенности запроса
Поиск точного соответствия	`entry_point.type = "web"` `correlated.verdict.priority = 10`	Имена полей чувствительны к регистру
	`entry_point.type = mail_bcc`	Строковые значения без специальных символов и пробелов можно писать без кавычек

	`user.is_anonymous = True`
	`user.is_anonymous = 1`
	`user.is_anonymous = False`
	`user.is_anonymous = 0`
		Логическое значение

Исключение определенного значения	`object.name != "archive.zip"`
	`entry_point.type != web`
	`correlated.verdict.priority != 10`
		Задания могут содержать несколько объектов. Если вы ищите задания по исключающим свойствам одного объекта, задание может попасть в результаты поиска по тем же свойствам, но найденным в другом объекте того же задания

Соответствие нескольким значениям	`correlated.verdict.threat.level IN (UNWANTED, DANGEROUS)`	—
Исключение нескольких значений	`entry_point.type NOT IN (web, mail_bcc)`	—
Поиск по неточным сравнениям (больше, меньше, равно)	`object.size > 1000` `object.size >= 100`	Поддерживаются суффиксы единиц измерения: KB, MB, GB, TB, PB. Если суффикс не указан, то считается, что размер указан в байтах
Вхождение в числовой диапазон	`object.size IN [1000..2000]` `object.size IN [1MB..2MB]`	

Доступные действия	Пример запроса	Особенности запроса

Поддерживаются поля с типом Дата	`start.date = 2021-01-01`
	`start.date > 2021-01-01`
	`start.date >= 2021-01-01`
		—

Поддерживаются поля с типом Время	`start > 2021-01-01 10:00:00` `start > 2021-01-01T10:00:00+0300`	В запросах используется время в часовом поясе пользователя. Можно явно указывать часовой пояс согласно формату ISO

Для полей с типом Время можно не указывать время и использовать только дату	`start > 2021-01-01`
	равно
	`start > 2021-01-01 00:00:00`
		—

Поиск по возрасту задания	`age > 3600`	Поддерживаются следующие единицы измерения: m, h, d, w, M. Если суффикс не указан, то считается, что возраст указан в секундах

Поиск текста по шаблону	`object.name ~ "*.pdf"`
	`object.name ~ "system*"`
	`object.name LIKE "%.DOC"`
		При использовании оператора LIKE искомое значение чувствительно к регистру

Поиск по всем текстовым полям сразу	`text ~ "*important*"`	—
Условия можно комбинировать, используя операторы AND (логическое И) и OR (логическое ИЛИ)	`age < 1h AND correlated.verdict.threat.level = DANGEROUS` `object.name ~ "*.pdf" OR object.name ~ "*.doc"`	Для операторов можно использовать любой регистр
Условия можно объединять скобками	`(age < 1h AND object.name ~ "*.pdf") OR (age < 30m AND object.name ~ "*.exe")`	Для операторов можно использовать любой регистр
К условию можно добавлять отрицание NOT	`NOT (object.name ~ "*.exe" OR object.name ~ "*.pdf")`	—

Доступные действия	Пример запроса	Особенности запроса
Сортировка результатов	`age > 1d ORDER BY entry_point.type, entry_point.id DESC`	После оператора указывается название поля, по которому нужно отсортировать результаты. После названия поля указывается ASC — если требуется сортировка по возрастанию значений, или DESC — если требуется сортировка по убыванию значений

В этом разделе

Поля для QL-запросов (см. раздел Б.1)

Типы вредоносного ПО (см. раздел Б.2)

Б.1. Поля для QL-запросов

В таблицах сгруппированы поля, которые вы можете использовать в QL-запросах для поиска заданий и объектов.

Общие поля

В таблице сгруппированы общие поля для поиска заданий и объектов.

Таблица 6. Общие поля

Поле	Тип данных	Описание
`age`	Integer	Возраст задания в секундах. В запросах вы можете использовать единицы измерения: `m` — минута, `h` — час, `d` — день, `w` — неделя, `M` — месяц, `Y` — год
`id, scan.id`	String	Идентификатор задания
`sandbox`	Boolean	Проверен ли объект методом поведенческого анализа. Это поле можно использовать только для поиска объектов
`start`	DateTime	Время создания задания
`start.date`	DateTime	Дата создания задания
`text`	String	Специальное поле для поиска по значениям всех текстовых полей

Поля для свойств задания

В таблице сгруппированы поля для поиска только заданий по их свойствам или результатам проверки.

Таблица 7. Поля для свойств задания

Поле	Тип данных	Описание
`action`	Enum	Решение о блокировке объекта: — `BLOCK` — заблокировать; — `NOTHING` — не требуется; — `PASS` — пропустить
`from_to`	String	Отправитель и получатель объекта (откуда — куда)
`quarantine.state`	Enum	Действие с заблокированными объектами задания: — `QUARANTINED` — помещены в карантин; — `REMOVED` — удалены
`status`	Enum	Статус обработки задания: — `FAIL` — отказ; — `SUCCESS` — успех
`task.object.name`	String	Название задания
`task.object.type`	Enum	Тип объекта задания: — `ARCHIVE` — архив; — `COMPRESSED_FILE` — сжатый файл; — `EMAIL` — письмо; — `EMAIL_BODY` — тело письма; — `FILE` — файл; — `FOLDER` — папка; — `HTTP` — HTTP-сообщение; — `SANDBOX_DROP` — dropped файл; — `SANDBOX_MEMORY_DUMP` — дамп памяти (memdump);

Поле	Тип данных	Описание
		— SANDBOX_PROCESS_MEMORY_DUMP — дамп памяти (procdump); — URL — ссылка
task.processed_at	DateTime	Дата и время решения о блокировке
task.processed_elapsed	Integer	Время от создания задания до решения о блокировке в секундах
task.threat.weight	Integer	Отрицательное число, характеризующее уровень опасности обнаруженной угрозы (чем больше, тем опасней). По модулю совпадает со значением task.correlated.verdict.priority. Используется для сортировки
task.verdict_at	DateTime	Дата и время вынесения вердикта
task.verdict_elapsed	Integer	Время от создания задания до вынесения вердикта в секундах
Результат проверки задания		
task.correlated.state	Enum	Статус проверки: — FULL — выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена
task.correlated.verdict.priority	Integer	Положительное число, характеризующее уровень опасности обнаруженной в задании угрозы (чем меньше, тем опасней). Три уровня для опасных объектов: 1—10, 11—40, 41—100. Три уровня для потенциально опасных: 101—115, 116—130, 131—199. Для безопасных — 200
task.correlated.verdict.threat.classification	Enum	Тип обнаруженного вредоносного ПО (см. раздел Б.2)
task.correlated.verdict.threat.family	String	Семейство угроз
task.correlated.verdict.threat.level	Enum	Степень опасности объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNWANTED — потенциально опасный

Поле	Тип данных	Описание
`task.correlated.verdict.threat.platform`	Enum	Платформа вредоносного ПО: — `ANDROID`; — `IOS`; — `LINUX`; — `NO_PLATFORM`; — `OSX`; — `WINDOWS`
Результат проверки задания методом поведенческого анализа		
`task.sandbox.correlated.state`	Enum	Статус проверки: — `FULL` — выполнена полностью; — `PARTIAL` — выполнена частично; — `UNSCANNED` — не выполнена
`task.sandbox.correlated.verdict.priority`	Integer	Положительное число, характеризующее уровень опасности угрозы, обнаруженной при поведенческом анализе (чем меньше, тем опасней). Три уровня для опасных объектов: 1—10, 11—40, 41—100. Три уровня для потенциально опасных: 101—115, 116—130, 131—199. Для безопасных — 200
`task.sandbox.correlated.verdict.threat.classification`	Enum	Тип обнаруженного вредоносного ПО (см. раздел Б.2)
`task.sandbox.correlated.verdict.threat.family`	String	Семейство угроз
`task.sandbox.correlated.verdict.threat.level`	Enum	Степень опасности объекта: — `CLEAN` — без обнаруженных угроз; — `DANGEROUS` — опасный; — `UNWANTED` — потенциально опасный
`task.sandbox.correlated.verdict.threat.platform`	Enum	Платформа вредоносного ПО: — `ANDROID`; — `IOS`; — `LINUX`;

Поле	Тип данных	Описание
		— NO_PLATFORM; — OSX; — WINDOWS

Поля с результатами проверки объекта

В таблице сгруппированы поля для поиска заданий и объектов по результатам проверки объектов.

Таблица 8. Поля с результатами проверки объекта

Поле	Тип данных	Описание
av.any.detections.name	String	Название угрозы, найденной антивирусами
av.any.detections.threat.classification	Enum	Тип вредоносного ПО по результатам проверки антивирусами (см. раздел Б.2)
bw_lists.errors.type	Enum	Название типа ошибки в черном или белом списке: — COLLISION_ERROR; — ENGINE_ERROR; — LISTS_NOT_READY_ERROR; — SCAN_MACHINE_ERROR; — TIMEOUT_ERROR
bw_lists.hashes	Enum	Тип хеш-суммы, по которой найдено совпадение в черном или белом списке: — MD5; — SHA1; — SHA256
bw_lists.state	Enum	Статус проверки: — FULL — выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена

Поле	Тип данных	Описание
bw_lists.status	Enum	Результат проверки по спискам: — IN_BLACK_LIST — в черном списке; — IN_WHITE_LIST — в белом списке; — NOT_IN_LISTS — отсутствует в списках
correlated.threat_source	Boolean	Является ли объект источником угрозы
correlated.state	Enum	Статус проверки: — FULL — выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена
correlated.verdict.priority	Integer	Положительное число, характеризующее уровень опасности объекта (чем меньше, тем опасней). Три уровня для опасных объектов: 1—10, 11—40, 41—100. Три уровня для потенциально опасных: 101—115, 116—130, 131—199. Для безопасных — 200
correlated.verdict.threat.classification	Enum	Тип обнаруженного вредоносного ПО (см. раздел Б.2)
correlated.verdict.threat.family	String	Семейство угроз
correlated.verdict.threat.level	Enum	Степень опасности объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNWANTED — потенциально опасный
correlated.verdict.threat.platform	Enum	Платформа вредоносного ПО: — ANDROID; — IOS; — LINUX; — NO_PLATFORM; — OSX; — WINDOWS
detections.name	String	Название обнаруженной угрозы

Поле	Тип данных	Описание
`detections.threat.classification`	Enum	Тип обнаруженного вредоносного ПО (см. раздел Б.2)
`threat.weight`	Integer	Отрицательное число, характеризующее уровень опасности обнаруженной угрозы (чем больше, тем опасней). По модулю совпадает со значением `correlated.verdict.priority`. Используется для сортировки
Результат проверки объекта определенным средством проверки		
В префиксе полей вы можете указывать следующие средства проверки: — `av.avast` — антивирус Avast Core Security; — `av.clamav` — антивирус Cisco Talos ClamAV; — `av.drweb` — антивирус Dr.Web Server Security Suite; — `av.kaspersky` — антивирус Kaspersky Web Traffic Security; — `av.nano` — антивирус NANO Security NANO; — `av.symantec` — антивирус Symantec Protection Engine for Network Attached Storage; — `ptesc` — средство статического анализа на основе YARA-правил PT ESC; — `ptioc` — средство обнаружения индикаторов компрометации PT IoC; — `rule_engine` — дополнительные критерии определения потенциально опасных файлов		
`<Средство проверки>.database.time`	DateTime	Дата и время обновления базы знаний средства проверки
`<Средство проверки>.database.version`	String	Версия базы знаний средства проверки
`<Средство проверки>.detections.is_apt`	Boolean	Обнаружены ли признаки целевой атаки
`<Средство проверки>.detections.is_exact`	Boolean	Является ли обнаружение точным
`<Средство проверки>.detections.name`	String	Название обнаруженной угрозы
`<Средство проверки>.detections.threat.classification`	Enum	Тип обнаруженного вредоносного ПО (см. раздел Б.2)
`<Средство проверки>.detections.threat.family`	String	Семейство угроз

Поле	Тип данных	Описание
`<Средство проверки>.detections.threat.platform`	Enum	Платформа вредоносного ПО: — `ANDROID`; — `IOS;` — `LINUX`; — `NO_PLATFORM`; — `OSX`; — `WINDOWS`
`<Средство проверки>.errors.type`	Enum	Название типа ошибки средства проверки: — `ANALYSIS_ERROR`; — `CONTAINS_CORRUPTED`; — `CONTAINS_ENCRYPTED`; — `CORRUPTED`; — `ENCRYPTED`; — `ENGINE_ERROR`; — `FILE_NOT_FOUND`; — `LIMIT_EXCEEDED`; — `SCAN_MACHINE_ERROR`; — `TIMEOUT_ERROR`; — `UNPACKING_ERROR`
`<Средство проверки>.state`	Enum	Статус проверки: — `FULL` — выполнена полностью; — `PARTIAL` — выполнена частично; — `UNSCANNED` — не выполнена
`<Средство проверки>.verdict.threat.classification`	Enum	Тип обнаруженного вредоносного ПО (см. раздел Б.2)
`<Средство проверки>.verdict.threat.family`	String	Семейство угроз

Поле	Тип данных	Описание
`<Средство проверки>.verdict.threat.level`	Enum	Степень опасности объекта: — `CLEAN` — без обнаруженных угроз; — `DANGEROUS` — опасный; — `UNWANTED` — потенциально опасный
`<Средство проверки>.verdict.threat.platform`	Enum	Платформа вредоносного ПО: — `ANDROID`; — `IOS`; — `LINUX`; — `NO_PLATFORM`; — `OSX`; — `WINDOWS`
`<Средство проверки>.version`	String	Версия средства проверки

Поля для свойства поведенческого анализа объектов

В таблице сгруппированы поля для поиска заданий и объектов по свойствам и результатам поведенческого анализа объектов.

Таблица 9. Поля для свойства поведенческого анализа объектов

Поле	Тип данных	Описание
`sandbox.behaviors.mitre_threat_id`	String	Идентификатор подозрительного поведения согласно базе знаний MITRE ATT&CK
`sandbox.behaviors.name`	String	Название подозрительного поведения
`sandbox.behaviors.weight`	Integer	Степень опасности подозрительного поведения объекта
`sandbox.bootkitmon`	Boolean	Выполнялась ли при поведенческом анализе перезагрузка ОС
`sandbox.bootkitmon_stage`	Enum	На каком этапе при поведенческом анализе с перезагрузкой ОС обнаружено вредоносное ПО: — `AFTER_REBOOT`; — `BEFORE_REBOOT`

Поле	Тип данных	Описание
sandbox.duration	Integer	Общая продолжительность поведенческого анализа в секундах
sandbox.errors.type	Enum	Тип ошибки, возникшей при поведенческом анализе: — ENGINE_ERROR; — FILE_NOT_FOUND; — INIT_ERROR; — NOT_ENOUGH_IMAGE_COPIES; — SCAN_MACHINE_ERROR; — TIMEOUT_ERROR; — UNKNOWN
sandbox.file_type	String	Тип проверенного файла
sandbox.image.name	String	Имя образа ВМ
sandbox.image.os.architecture	String	Архитектура образа ВМ
sandbox.image.os.locale	String	Локализация образа ВМ
sandbox.image.os.name	String	Название ОС образа ВМ
sandbox.image.os.service_pack	String	Версия пакета образа ВМ
sandbox.image.os.version	String	Версия ОС образа ВМ
sandbox.image.version	String	Версия образа ВМ
sandbox.init_msdn_error.code	Integer	Код ошибки MSDN
sandbox.init_msdn_error.name	String	Имя ошибки MSDN
sandbox.item.process.name	String	Имя процесса из поведенческого анализа
sandbox.item.trigger	String	Триггер снятия дампа объекта поведенческого анализа
sandbox.mitm	Boolean	Была ли при поведенческом анализе включена подмена сертификатов ПО сертификатами PT Sandbox для расшифровки и анализа защищенного трафика

Поле	Тип данных	Описание
sandbox.planned_duration	Integer	Планируемая продолжительность поведенческого анализа в секундах
sandbox.produced	Boolean	Фильтр по объектам поведенческого анализа
sandbox.rules_version.correlation	String	Версия правил корреляции поведенческого анализа
sandbox.rules_version.dpi	String	Версия правил DPI поведенческого анализа
sandbox.state	Enum	Статус проверки: — FULL — выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена
Результат поведенческого анализа объекта		
sandbox.detections.name	String	Название обнаруженной угрозы
sandbox.detections.threat.classification	Enum	Тип обнаруженного вредоносного ПО (см. раздел Б.2)
sandbox.detections.threat.family	String	Семейство угроз
sandbox.detections.threat.platform	Enum	Платформа вредоносного ПО: — ANDROID; — IOS; — LINUX; — NO_PLATFORM; — OSX; — WINDOWS
sandbox.verdict.threat.classification	Enum	Тип обнаруженного вредоносного ПО (см. раздел Б.2)
sandbox.verdict.threat.family	String	Семейство угроз
sandbox.verdict.threat.level	Enum	Степень опасности объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNWANTED — потенциально опасный

Поле	Тип данных	Описание
sandbox.verdict.threat.platform	Enum	Платформа вредоносного ПО: — ANDROID; — IOS; — LINUX; — NO_PLATFORM; — OSX; — WINDOWS
Результат по всем артефактам поведенческого анализа		
sandbox.correlated.state	Enum	Статус проверки: — FULL — выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена
sandbox.correlated.verdict.threat.classification	Enum	Тип обнаруженного вредоносного ПО (см. раздел Б.2)
sandbox.correlated.verdict.threat.family	String	Семейство угроз
sandbox.correlated.verdict.threat.level	Enum	Степень опасности объекта: — CLEAN — без обнаруженных угроз; — DANGEROUS — опасный; — UNWANTED — потенциально опасный
sandbox.correlated.verdict.threat.platform	Enum	Платформа вредоносного ПО: — ANDROID; — IOS; — LINUX; — NO_PLATFORM; — OSX; — WINDOWS

Поля для свойств объекта

В таблице сгруппированы поля для поиска заданий и объектов по свойствам объектов.

Таблица 10. Поля для свойств объекта

Поле	Тип данных	Описание
`ancestor.node_id`	Integer	Идентификатор дочернего объекта в карточке задания. Это поле можно использовать только для поиска объектов
`errors.type`	Enum	Тип ошибки, возникшей при проверке: — `ANALYSIS_ERROR`; — `CONNECT_TIMEOUT`; — `CONTAINS_CORRUPTED`; — `CONTAINS_ENCRYPTED`; — `CORRUPTED`; — `ENCRYPTED`; — `ENGINE_ERROR`; — `FILE_NOT_FOUND`; — `INIT_ERROR`; — `LIMIT_EXCEEDED`; — `MAX_REDIRECT_EXCEEDED`; — `MAX_SIZE_EXCEEDED`; — `NOT_ENOUGH_IMAGE_COPIES`; — `NOT_FILE`; — `NO_SUITABLE_UNPACKER`; — `READ_TIMEOUT`; — `SCAN_MACHINE_ERROR`; — `TIMEOUT_ERROR`; — `UNKNOWN`; — `UNPACKING_ERROR`
`network_objects.any`	String	Значение сетевого артефакта
`network_objects.url`	String	Значение сетевого артефакта с типом URL

Поле	Тип данных	Описание
`node.type`	Enum	Тип элемента в карточке задания: — `ARTIFACT` — карточка объекта; — `SANDBOX` — карточка поведенческого анализа; — `SANDBOX_STAGE` — карточка поведенческого анализа с перезагрузкой
`object.file_type`	String	Тип файла, определенный PT ESC
`object.from_cache`	Boolean	Получен ли объект из кэша
`object.md5`	String	Хеш-сумма MD5 объекта
`object.mime_type`	String	MIME-тип объекта
`object.name`	String	Имя объекта
`object.properties`	Enum	Свойства объекта: — `ARCHIVE` — архив; — `COMPRESSED` — сжатый файл; — `EMAIL` — письмо; — `ENCRYPTED` — зашифрованный; — `HAS_ACTION` — содержит Action; — `HAS_ACTIVE_X` — с элементами ActiveX; — `HAS_DDE` — с функциями DDE; — `HAS_EMBEDDED` — с OLE-объектами; — `HAS_JAVASCRIPT` — содержит JavaScript; — `HAS_MACROS` — с макросами; — `HAS_OPEN_ACTION` — содержит OpenAction; — `HAS_REMOTE_DATA` — с запросами к внешним данным; — `HAS_REMOTE_TEMPLATE` — использует внешний шаблон; — `MULTI_VOLUME` — многотомный архив; — `OFFICE` — файл офисного формата; — `SFX` — самораспаковывающийся архив
`object.sha1`	String	Хеш-сумма SHA-1 объекта

Поле	Тип данных	Описание
`object.sha256`	String	Хеш-сумма SHA-256 объекта
`object.size`	Integer	Размер объекта в байтах. В запросах вы можете использовать единицы измерения `KB`, `MB`, `GB`, `TB`, `PB`
`object.type`	Enum	Тип объекта: — `ARCHIVE` — архив; — `COMPRESSED_FILE` — сжатый файл; — `EMAIL` — письмо; — `EMAIL_BODY` — тело письма; — `FOLDER` — папка; — `FILE` — файл; — `HTTP` — HTTP-сообщение; — `SANDBOX_DROP` — dropped файл; — `SANDBOX_MEMORY_DUMP` — дамп памяти (memdump); — `SANDBOX_PROCESS_MEMORY_DUMP` — дамп памяти (procdump); — `URL` — ссылка
`parent.node_id`	Integer	Идентификатор родительского объекта в карточке задания. Это поле можно использовать только для поиска объектов
`unpacker.errors.type`	Enum	Тип ошибки распаковщика: — `CORRUPTED`; — `ENCRYPTED`; — `ENGINE_ERROR`; — `FILE_NOT_FOUND`; — `LIMIT_EXCEEDED`; — `NO_SUITABLE_UNPACKER`; — `SCAN_MACHINE_ERROR`; — `TIMEOUT_ERROR`; — `UNKNOWN`

Поле	Тип данных	Описание
`unpacker.state`	Enum	Статус распаковки: — `FULL` — выполнена полностью; — `PARTIAL` — выполнена частично; — `UNSCANNED` — не выполнена
Свойства письма		
`email.bcc.address`	String	Почтовый адрес получателя скрытой копии (BCC)
`email.bcc.name`	String	Имя получателя скрытой копии (BCC)
`email.cc.address`	String	Почтовый адрес получателя копии (CC)
`email.cc.name`	String	Имя получателя копии (CC)
`email.from.address`	String	Почтовый адрес отправителя
`email.from.name`	String	Имя отправителя
`email.id`	String	Идентификатор письма
`email.subject`	String	Тема письма
`email.to.address`	String	Почтовый адрес получателя
`email.to.name`	String	Имя получателя
`envelope.from`	String	Адрес отправителя (в транспортных заголовках)
`envelope.recipients`	String	Адреса получателей (в транспортных заголовках)
`envelope.result.action`	Enum	Решение о блокировке исходного письма: — `BLOCK` — заблокировать; — `NOTHING` — не требуется; — `PASS` — пропустить
`envelope.result.delivery_status`	Enum	Статус доставки исходного письма: — `FAIL` — не доставлено; — `SKIP` — неизвестен; — `SUCCESS` — доставлено
`envelope.result.email_type`	Enum	Тип исходного письма: — `DISARMED` — обезвреженное письмо; — `NOTHING` — ничего;

Поле	Тип данных	Описание
		— NOTIFICATION — уведомление; — SOURCE — исходное письмо
envelope.result.recipient	String	Адрес получателя в исходном письме
Свойства ссылки		
download_url.engine_version	String	Версия средства для скачивания контента по ссылкам
download_url.errors.type	Enum	Тип ошибки, возникшей при проверке ссылки: — CONNECT_TIMEOUT; — ENGINE_ERROR; — FILE_NOT_FOUND; — MAX_REDIRECT_EXCEEDED; — MAX_SIZE_EXCEEDED; — NOT_FILE; — READ_TIMEOUT; — SCAN_MACHINE_ERROR; — TIMEOUT_ERROR; — UNKNOWN
download_url.state	Enum	Статус проверки ссылки: — FULL — выполнена полностью; — PARTIAL — выполнена частично; — UNSCANNED — не выполнена
source.crawler.engine_name	Enum	Тип средства для скачивания контента по ссылкам: — CURL; — WEB_ENGINE
source.crawler.url	String	Ссылка, по которой скачан файл
url	String	URL
url.redirects.status	Integer	HTTP-статусы перенаправлений
url.redirects.url	String	URL перенаправлений

Свойства источников

В таблице сгруппированы поля для поиска заданий и объектов по свойствам источников объектов.

Таблица 11. Свойства источников

Поле	Тип данных	Описание
`entry_point.id`	String	Идентификатор источника
`entry_point.name`	String	Название источника
`entry_point.type`	Enum	Тип источника: — `CHECK_ME` — служба Checkme; — `FILE_INBOX` — папка-шлюз; — `FILE_MONITOR` — общая папка; — `ICAP` — ICAP-сервер; — `INTERACTIVE_ANALYSIS` — веб-интерфейс (ручной поведенческий анализ); — `MAIL_AGENT` — почтовый сервер с установленным агентом; — `MAIL_BCC` — почтовый сервер в режиме зеркалирования; — `MAIL_GATEWAY` — почтовый сервер в режиме фильтрации; — `PTNAD` — PT NAD; — `PUBLIC_API` — API с передаваемыми параметрами проверки; — `RETRO` — хранилище файлов (ретроспективный анализ); — `SCAN_API` — API с выбранными параметрами проверки; — `WEB` — веб-интерфейс
`file_inbox.dst`	String	Папка назначения
`file_inbox.src`	String	Исходная папка-шлюз
`file_monitor.src`	String	Исходная общая папка
`web.referer`	String	HTTP Referer

Поле	Тип данных	Описание
web.user_agent	String	HTTP User-Agent
web.x_forwarded_for	String	Значение заголовка X-Forwarded-For
Веб-интерфейс		
user.id	String	Идентификатор пользователя
user.is_anonymous	Boolean	Является ли пользователь анонимным
user.login	String	Логин пользователя
user.name	String	Имя пользователя
ICAP-сервер		
icap.client.ip	String	IP-адрес ICAP-клиента
icap.client.username	String	Имя пользователя ICAP-клиента
icap.method	String	Метод ICAP
icap.url	String	URL ICAP
icap.version	String	Версия ICAP
PT NAD		
ptnad.dst.ip	String	IP-адрес назначения
ptnad.dst.port	Integer	Порт назначения
ptnad.http.host	String	HTTP Host
ptnad.http.referer	String	HTTP Referer
ptnad.http.uri	String	HTTP URI
ptnad.http.user_agent	String	HTTP User-Agent
ptnad.proto	String	Протокол
ptnad.src.ip	String	Исходный IP-адрес
ptnad.src.port	Integer	Исходный порт

Б.2. Типы вредоносного ПО

В таблице указаны возможные значения полей для поиска по типам вредоносного ПО.

Таблица 12. Типы вредоносного ПО

Значение	Тип	Описание
ADWARE	Рекламное ПО	Программное обеспечение, распространяемое в рекламных целях. Незаметно попав на устройство, оно демонстрирует пользователю рекламу, а также собирает пользовательскую информацию для партнерских программ. Может вводить владельца устройства в заблуждение для легитимизации своего присутствия
BACKDOOR	Бэкдор	Вредоносное ПО для скрытого удаленного управления устройством. Представители этого класса — неотъемлемая часть целевых атак
BOOTKIT	Буткит	Вредоносное ПО, запускающее вредоносный код на самых ранних этапах загрузки ОС
CLIENT_IRC	IRC-клиент	Программа, используемая для коммуникации в IRC (Internet Relay Chat), обмена файлами и управляющими командами с применением нестандартного протокола связи. Не является вредоносной, но может быть использована злоумышленниками
CLIENT_P2P	P2P-клиент	Программа, используемая для работы с peer-to-peer-сетями. Применяется для обмена информацией в распределенной архитектуре хранения и передачи данных. Не является вредоносной, но может быть использована злоумышленниками
CLIENT_SMTP	SMTP-клиент	Программа, используемая для отправки электронных писем в скрытом режиме. Чаще применяется в составе многофункционального ПО. Не является вредоносной, но может быть использована злоумышленниками
CONSTRUCTOR	Конструктор	Программа для сборки новых образцов вредоносного ПО. Злоумышленники используют ее при подготовке к атаке. Продается на теневых форумах
DIALER	Средство дозвона	Программа, используемая для установки телефонных соединений в скрытом режиме. Не является вредоносной, но может быть использована злоумышленниками
DOS	DoS-утилита	Программа для проведения атаки типа «отказ в обслуживании». При отправке большого числа запросов принимающая сторона не успевает их обработать и становится временно недоступной. Может использоваться для выведения из строя средств защиты

Значение	Тип	Описание
DOWNLOADER	Загрузчик	Программа для скрытого скачивания данных из сетевых источников. Чаще применяется в составе многофункционального ПО. Не является вредоносной, но может быть использована злоумышленниками
EMAIL_FLOODER	Почтовый спамер	Программа для отправки большого количества бесполезной информации с помощью электронной почты. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
EMAIL_WORM	Почтовый червь	Вредоносное ПО, способное распространяться с помощью электронных писем
EXPLOIT	Эксплойт	Вредоносное ПО, использующее для развития атаки одну или несколько уязвимостей в целевом ПО. Применяется для запуска вредоносного кода без участия пользователя. Злоумышленники могут использовать его для повышения привилегий на устройстве
FLOODER	Флудильщик	Программа для отправки большого количества бесполезной информации по сетевым каналам. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
FRAUDTOOL	Инструмент для мошенничества	Программа, которая не выполняет заявленных функций. Может отвлекать пользователя или вводить его в заблуждение. Не является вредоносной, но может быть использована злоумышленниками
HACKTOOL	Пентест-инструменты	Инструмент, помогающий злоумышленнику развить атаку. Может использоваться для изменения параметров устройства, чтобы ослабить его защищенность, или для сокрытия действий атакующего. Применяется в тестировании на проникновение
HOAX	Программа-розыгрыш	Программа, предназначенная для демонстрации пользователю ложной, пугающей информации. Может злоупотреблять ресурсами ОС, причиняя неудобства и побуждая владельца устройства к необдуманным действиям (чаще всего злоумышленники используют такое ПО, чтобы обманом получить деньги пользователя)
IM_FLOODER	IM-флудильщик	Программа для отправки большого количества бесполезной информации через мессенджеры. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты

Значение	Тип	Описание
IM_WORM	IM-червь	Вредоносное ПО, способное распространяться через мессенджеры
IRC_WORM	IRC-червь	Вредоносное ПО, способное распространяться через IRC (Internet Relay Chat)
MONITOR	Средство мониторинга	Программа для наблюдения за действиями пользователя. Применяется для трассировки активности ОС. Не является вредоносной, но может быть использована злоумышленниками
NET_WORM	Сетевой червь	Вредоносное ПО, способное распространяться без участия пользователя. Для этого используются уязвимости в ПО на новых узлах сети с последующим запуском вредоносного кода
NETTOOL	Сетевая утилита	Инструмент, выполняющий действия над сетевыми ресурсами в IT-инфраструктуре. Не является вредоносным ПО, чаще всего используется для сетевого администрирования, но злоумышленники могут применять его для развития атак
P2P_WORM	P2P-червь	Вредоносное ПО, способное распространяться через пиринговые сети
PHISHING	Фишинг	Рассылка с вредоносным содержимым, распространяемая через электронные письма или сообщения в мессенджерах. Злоумышленник обманным путем заставляет пользователя открыть присланный файл или перейти по ссылке. Если цель фишинга — кража средств, текст сообщения может содержать побуждение к выполнению денежных операций
PSWTOOL	Средство восстановления паролей	Программа для получения учетных данных пользователя и восстановления утраченной информации. Не является вредоносной, но может быть использована злоумышленниками
REMOTEADMIN	Средство удаленного доступа	Программа для удаленного управления устройством. Применяется для демонстрации действия пользователя или оказания услуг технической поддержки. Не является вредоносной, но может быть использована злоумышленниками
RISKTOOL	Потенциально нежелательное ПО	Инструмент для работы с локальными ресурсами устройства пользователя. Не является вредоносным ПО и чаще всего применяется для администрирования ОС, но, попав в руки злоумышленников, может нанести вред пользовательским данным

Значение	Тип	Описание
ROOTKIT	Руткит	Вредоносное ПО для сокрытия в системе объектов либо действий злоумышленника
SERVER_FTP	FTP-сервер	Удаленный компьютер, выполняющий функции FTP-сервера. Применяется для получения удаленного доступа к хранилищу данных на устройстве. Не является вредоносным ПО, но может быть использован злоумышленниками
SERVER_PROXY	Прокси-сервер	Удаленный компьютер, выполняющий функции прокси-сервера. Применяется для передачи данных через промежуточные узлы, когда пользователю нужно оставаться анонимным или отсутствует доступ к какой-либо сети. Не является вредоносным ПО, но может быть использован злоумышленниками
SERVER_TELNET	Telnet-сервер	Удаленный компьютер, выполняющий функции Telnet-сервера. Применяется для получения удаленного доступа к устройству пользователя. Не является вредоносным ПО, но может быть использован злоумышленниками
SERVER_WEB	Веб-сервер	Удаленный компьютер, выполняющий функции веб-сервера. Применяется для назначения устройству роли управляющего узла либо для получения доступа к информации. Не является вредоносным ПО, но может быть использован злоумышленниками
SMS_FLOODER	СМС-флудильщик	Программа для отправки большого количества бесполезной информации через SMS-сообщения. Может быть использована для рассылки спама, отвлечения внимания пользователя или обхода средств защиты
SPAM	Спам	Электронное письмо в составе массовой рассылки. Чаще всего содержит рекламное сообщение. Не несет ценной информации для пользователя
SPOOFER	Подмена	Программа для подмены идентификатора отправителя при отправке сетевых запросов. Применяется, чтобы сокрыть адрес атакующего, помочь ему избежать обнаружения или легитимизировать выполняемые действия
TROJAN	Троян	Вредоносное ПО для совершения нелегитимных действий на устройстве пользователя (их невозможно классифицировать более точно). Не имеет возможностей для самораспространения

Значение	Тип	Описание
TROJAN_ARCBOMB	Архивная бомба	Вредоносное ПО, представляющее собой архив, при распаковке которого большая доля свободного пространства жесткого диска заполняется бесполезными или пустыми данными. Это может привести к замедлению работы устройства или к прекращению работы некоторых программ
TROJAN_BANKER	Банковский троян	Вредоносное ПО для кражи учетных данных пользователя, связанных с финансовыми системами, и передачи полученной информации злоумышленнику
TROJAN_CLICKER	Троян-кликер	Вредоносное ПО, симулирующее обращения к интернет-ресурсам. Используется для искусственной накрутки счетчиков посещений сайта с целью продвижения ресурса либо монетизации
TROJAN_DDOS	DDoS-бот	Вредоносное ПО для проведения распределенных атак типа «отказ в обслуживании». Компьютер пользователя автоматически становится звеном атаки. Злоумышленники могут настраивать ПО, чтобы изменить перечень целевых ресурсов
TROJAN_DOWNLOADER	Загрузчик ВПО	Вредоносное ПО для скачивания и запуска другого вредоносного ПО. Наиболее часто используемый класс вредоносного ПО для первичного заражения устройства
TROJAN_DROPPER	Установщик ВПО	Вредоносное ПО, извлекающее из своего тела и запускающее другое вредоносное ПО. Зачастую такая программа может установить вредоносное ПО нескольких классов
TROJAN_FAKEAV	Лжеантивирус	Вредоносное ПО, представляемое пользователю в качестве антивирусного продукта, но не являющееся таковым. Может требовать плату за использование, блокировать работу устройства, нарушать функционирование системы
TROJAN_GAMETHIEF	Средство кражи игровых учетных данных	Вредоносное ПО для кражи пользовательских данных в компьютерных и мобильных играх и передачи полученной информации злоумышленнику
TROJAN_IM	Средство кражи учетных	Вредоносное ПО для кражи пользовательских данных в мессенджерах и передачи полученной информации злоумышленнику

Значение	Тип	Описание
	данных мессенджеров	
TROJAN_MAILFINDER	Сборщик адресов электронной почты	Вредоносное ПО для сбора адресов электронной почты с устройства пользователя и передачи их злоумышленнику
TROJAN_NOTIFIER	Троян-уведомитель	Вредоносное ПО, уведомляющее злоумышленника об успешном заражении устройства. Не получает от злоумышленника дополнительных компонентов или команд
TROJAN_PROXY	Троян-прокси	Вредоносное ПО, предоставляющее злоумышленнику анонимный доступ в интернет через устройство пользователя либо туннелирующее сетевой трафик до недоступных извне узлов сети. Часто используется на стадии горизонтального перемещения либо для извлечения важных данных при проведении атак
TROJAN_PSW	Средство кражи учетных данных	Вредоносное ПО для кражи учетных данных пользователя в системе или других программах и передачи полученной информации злоумышленнику
TROJAN_RANSOM	Троян-вымогатель	Вредоносное ПО для вымогательской деятельности. Ценные файлы владельца устройства шифруются, а за их восстановление предлагается заплатить выкуп. В некоторых случаях те же файлы передаются злоумышленнику, чтобы усилить давление на пользователя и повысить шанс оплаты
TROJAN_SMS	СМС-троян	Вредоносное ПО для отправки SMS-сообщений на номера, которые определяет злоумышленник. Может использоваться для подписки пользователя на платные сервисы
TROJAN_SPY	Программа-шпион	Вредоносное ПО для отслеживания действий пользователя (перехват нажатых клавиш на клавиатуре, получение изображения экрана, истории используемых программ, аудиозапись разговоров) и передачи полученной информации злоумышленнику
UNKNOWN	—	Угроз не обнаружено
UNKNOWN_THREAT	—	Тип вредоносного ПО не указан

Значение	Тип	Описание
VIRTOOL	ПО для создания вирусов	Программа, которую злоумышленники используют для модификации вредоносного ПО, чтобы скрыть его от средств защиты. Применяются методы обфускации кода, шифрования данных или стеганографии. Может использоваться для заражения легитимного ПО
VIRUS	Вирус	Вредоносное ПО, способное распространяться среди локальных ресурсов пользователя
WEBTOOLBAR	Панель инструментов браузера	Панель инструментов, расширяющая возможности браузера. Иногда может получать доступ к значимым данным пользователя либо добавлять нежелательные возможности. Не является вредоносным ПО, но может быть использована злоумышленниками
WORM	Компьютерный червь	Вредоносное ПО, способное распространяться среди сетевых ресурсов пользователя

Глоссарий

анонимная проверка

Проверка объектов через веб-интерфейс без аутентификации в продукте.

вердикт

Решение продукта о наличии или отсутствии угрозы в объекте, уровне опасности этой угрозы и типе представляющего угрозу вредоносного ПО.

динамический анализ

Совокупность методов проверки объекта, основанных на анализе его поведения. Имитируется взаимодействие пользователя с объектом и отслеживается появление связанных с этим угроз.

дочерний объект

Объект, выделенный продуктом из другого объекта. Например, при распаковке архива, извлечении ссылок из письма или скачивании контента по ссылке.

задание на проверку

Совокупность информации, связанной с действиями продукта по выявлению угроз в поступивших на проверку объектах.

индикатор компрометации

Объект или свойство объекта, которые указывают на связь рассматриваемой активности в сети организации с известными угрозами ИБ. Индикаторами компрометации могут быть, например, хеш-суммы файлов, доменные имена или IP-адреса.

карточка задания

Страница в интерфейсе продукта с информацией о задании на проверку. На странице отображается информация об обнаруженных в задании угрозах и вынесенном по заданию вердикте.

карточка объекта

Страница в интерфейсе продукта с информацией об объекте задания. На странице отображается информация об используемых методах проверки, обнаруженных угрозах и вынесенном по объекту вердикте.

карточка поведенческого анализа

Страница в интерфейсе продукта с информацией о проверке файла задания методом поведенческого анализа.

наследуемый вердикт

Вердикт, вынесенный на основании результатов проверки дочерних объектов.

объект

Выделенный продуктом или полученный извне объем данных, для которого выполняется проверка на наличие угрозы. Например, файл, архив, письмо или ссылка.

опасный объект

Объект, который является вредоносным ПО и представляет угрозу для информационной системы или данных организации.

поведенческий анализ

Метод проверки объекта, основанный на анализе его поведения в изолированной виртуальной среде. Для выявления угроз в изолированной ОС имитируется взаимодействие пользователя с объектом и отслеживаются изменения, вносимые объектом в ОС и установленное ПО.

потенциально опасный объект

Объект, который при определенных обстоятельствах или действиях пользователя может представлять угрозу для информационной системы или данных организации.

прямой вердикт

Вердикт, вынесенный на основании результатов проверки самого объекта.

ретроспективный анализ

Метод проверки, заключающийся в регулярной повторной проверке объектов в хранилище. Использование обновленных средств проверки и антивирусных баз позволяет выявлять ранее неизвестные угрозы в уже проверенных объектах.

статический анализ

Совокупность методов проверки объектов, основанных на анализе их свойств и содержимого.

угроза

Возможность того, что информационной системе или данным организации будет нанесен вред. Угроза исходит от опасных и потенциально опасных объектов.