kaspersky

Kaspersky Threat Attribution Engine

Руководство по внедрению

Версия приложения: 1.0

kaspersky

Содержание

О Kaspersky Threat Attribution Engine

В этом разделе описывается программа Kaspersky Threat Attribution Engine и ее назначение.

Как работает Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine автоматически анализирует «генетику» вредоносных программ на предмет сходства кода с ранее исследованными образцами развитых устойчивых угроз (Advanced Persistent Threat, APT) и связанными объектами атрибуции. Он сравнивает «генотипы» (небольшие двоичные фрагменты анализируемых файлов) с базой данных образцов вредоносных программ APT и предоставляет отчет о происхождении вредоносных программ, объектах атрибуции и сходстве файлов с известными образцами APT.

Кроме того, продукт позволяет группам безопасности добавлять частные объекты и объекты атрибуции в свою базу данных и обучать продукт атрибуции образцов, аналогичных файлам в вашей частной коллекции. С помощью механизма атрибуции угроз процесс атрибуции занимает всего несколько секунд по сравнению с годами, которые требовались в прошлом.

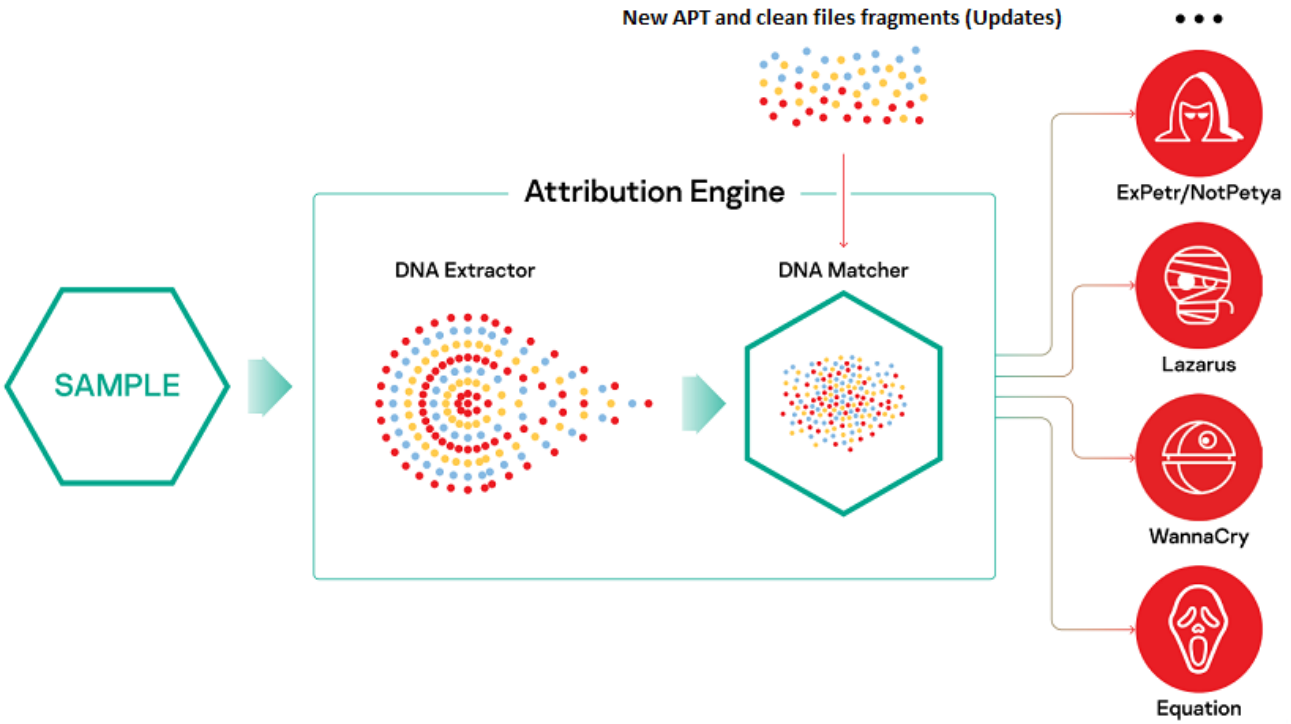

Рисунок 1: Рабочий процесс Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine извлекает соответствующие генотипы, отвечающие определенным критериям, и вычисляет репутацию выборки. Он раскрывает генотип образца и атрибуцию кода, давая вам представление о происхождении вредоносного ПО и его возможных авторах.

Назначение Kaspersky Threat Attribution Engine

Программа Kaspersky Threat Attribution Engine предназначена для атрибуции угроз и не может использоваться для обнаружения вредоносного ПО и киберугроз.

kaspersky

Все результаты, полученные при использовании Kaspersky Threat Attribution Engine и созданные в процессе анализа информации, предоставленной Kaspersky Threat Attribution Engine, носят оценочный характер и не могут считаться доказательствами или использоваться в качестве доказательств.

Угрозы и объекты атрибуции, классифицируемые Kaspersky Threat Attribution Engine как развитые устойчивые угрозы (APT), не обязательно могут быть классифицированы пользователем как APT. Все результаты, предоставляемые Kaspersky Threat Attribution Engine, носят оценочный характер. Пользователь должен принять окончательное решение о статусе любого образца или объекта атрибуции.

В этой главе

Требования к оборудованию и программному обеспечению

В этом разделе описаны системные требования Kaspersky Threat Attribution Engine.

Требования безопасности

Kaspersky Threat Attribution Engine предъявляет следующие требования к безопасности:

- USB-токен с ключами шифрования. Этот токен должен быть подключен к серверу, на котором будет работать Kaspersky Threat Attribution Engine.
- Сертификат сервера (по умолчанию используется самозаверенный сертификат).

Поддерживаемые операционные системы

Kaspersky Threat Attribution Engine может работать в операционной системе CentOS 7

Требования к ПО

Kaspersky Threat Attribution Engine предъявляет следующие требования к программному обеспечению:

- Командный процессор Bash.
- Openssl.
- MySQL версии 8.0.18-1 или выше.
- java-1.8.0-openjdk.
- pcsc-lite.
- Usbutils.
- компилятор libGCC.
- Библиотека GLIBC версии 2.3.6 или выше.

Поддерживаемые браузеры

Kaspersky Threat Attribution Engine поддерживает последние версии следующих браузеров:

- Mozilla Firefox.
- Google Chrome.
- Safari.
- Microsoft Edge.
- Chromium.

Требования к процессору

Для Kaspersky Threat Attribution Engine требуется процессор Intel® Xeon® 2,2 ГГц (10C / 20T) или более быстрый (или аналогичный).

Требования к ОЗУ и месту на жестком диске

Kaspersky Threat Attribution Engine требует 128 гигабайт (ГБ) оперативной памяти.

Kaspersky Threat Attribution Engine требует 8 ТБ SSD на жестком диске. При интенсивном чтении рекомендуется RAID5 с контролем четности + резервный.

Комплект поставки

В этом разделе описывается дистрибутив программы Kaspersky Threat Attribution Engine.

О дистрибутиве

В дистрибутив Kaspersky Threat Attribution Engine входят следующие файлы и элементы:

- Пакет RPM.
- Файл с лицензионным ключом для Kaspersky DeepUnpack.
- Набор файлов, содержащих информацию базы данных.
- Токен.
- Скрипты установки.

kaspersky

Файлы дистрибутива

Дистрибутив содержит следующие файлы и директории.

Таблица 1. Состав дистрибутива

Объект	Описание
bin/ktae_%version%.rpm	RPM-пакет с Kaspersky Threat Attribution Engine.
bin/SafenetAuthenticationClient-9.1.7-0.x86_64.rpm	Пакет RPM с драйвером Safenet для токена.
conf/application.conf	Файл конфигурации с параметрами службы по умолчанию.
conf/my.conf	Файл конфигурации MySQL с рекомендованными параметрами.
conf/settings.deepunpack.xml	Конфигурационный файл.
conf/settings.ktae.xml	Конфигурационный файл.
license/appinfo.kli	Сервисный файл с лицензионной информацией.
license/license.key	Файл лицензионного ключа DeepUnpack.
scripts/sql/create_schema_and_user.sql	SQL-скрипт, используемый во время установки.
scripts/sql/discard_tablespaces.sql	SQL-скрипт, используемый во время установки.
scripts/sql/drop_schema_and_user.sql	SQL-скрипт, используемый во время установки.
scripts/sql/import_tablespaces.sql	SQL-скрипт, используемый во время установки.
scripts/check_installation.sh	Сценарий оболочки, используемый во время установки.
scripts/check_installed_packages.sh	Сценарий оболочки, используемый во время установки.
scripts/drop_db.sh	Сценарий оболочки, который удалил базу данных для повторной инициализации.
scripts/generate_ssl_certificate.sh	Сценарий оболочки, используемый во время установки.
scripts/install_ktae.sh	Сценарий оболочки, используемый во время установки.
scripts/install_safenet_driver.sh	Сценарий оболочки, используемый во время установки.
txt/ktae_data_md5s.txt	Файл, содержащий хеши MD5 файлов, содержащих данные базы данных.
install_ktae_updater.sh	Сценарий оболочки, который устанавливает службу Updater во время установки.
00_install_dependencies.sh	Сценарий оболочки, устанавливающий зависимости во время установки.
01_install_ktae.sh	Shell-скрипт, устанавливающий Kaspersky Threat Attribution Engine во время установки.
02_run_ktae.sh	Сценарий оболочки, запускающий Kaspersky Threat Attribution Engine во время установки.
03_discard_db_tables.sh	Сценарий оболочки, который подготавливает таблицы базы данных для импорта во время установки.
04_copy_db_tables.sh	Сценарий оболочки, который копирует файлы базы данных в директорию MySQL во время установки.

05_import_db_tables.sh	Сценарий оболочки, который импортирует таблицы базы данных из скопированных файлов базы данных.
Kaspersky Threat Attribution Engine.pdf	Документация Kaspersky Threat Attribution Engine.

Директория Kaspersky Threat Attribution Engine

Во время установки следующие файлы извлекаются в директорию `/ opt / ktae`.

Таблица 2. Содержимое директории Kaspersky Threat Attribution Engine

Объект	Описание
bin/service	Исполняемый файл Kaspersky Threat Attribution Engine
bin/admin_cli	Утилита администрирования
cert/server.p12	Сертификат сервера
conf/application.conf	Конфигурационный файл
conf/application.ini	Конфигурационный файл
conf/logback.xml	Конфигурационный файл
deepunpack/*	Директория с файлами DeepUnpack
docs/legal_notices.txt	Юридическая информация о продукте
docs/license_KTAE_1_0_0_en.rtf	Лицензионное соглашение с конечным пользователем (EULA)
docs/release_notes_KTAE_1.0.0.pdf	Примечания к выпуску
docs/userguide/*	Документация в формате HTML
extracted (empty directory)	Директория извлеченных генотипов и строк
kavehost/*	Директория со служебными файлами kavehost. Этот сервис используется DeepUnpack.
lib/*	Вспомогательные библиотеки.
logs/logFile.txt	Файл с журналами Kaspersky Threat Attribution Engine
share/*	Директория для файлов, распакованных DeepUnpack
tools/linux/binutils/strings	Утилита для извлечения генотипов и строк
tools/linux/genotype	Утилита для извлечения генотипов и строк
uploaded (empty directory)	Директория для загруженных файлов

Директория обновления

Во время установки в директорию `/ opt / ktae-updater` извлекаются следующие файлы.

Таблица 3. Содержимое директории Kaspersky Threat Attribution Engine Updater

Объект	Описание
bases/*	Директория для загруженных файлов базы данных
bin/downloads/bases_tmp/ (empty directory)	Директория для временных файлов базы данных
bin/downloads/tmp/ (empty directory)	Директория для временных файлов
bin/appinfo.kli	Сервисный файл с лицензионной информацией
bin/keepup2date8	Бинарный файл службы обновления
bin/keepup2date8.sh	Скрипт, запускающий службу Updater
bin/license.key	Файл лицензионного ключа DeepUnpack
bin/settings.xml	Конфигурационный файл
bin/upsdk.xml	Конфигурационный файл
docs/legal_notices.txt	Юридические уведомления для службы обновления
lib/*	Вспомогательные библиотеки
download_all.sh	Сценарий оболочки, скачивающий обновления
download.sh	Сценарий оболочки, скачивающий обновления
settings.deepunpack.xml	Конфигурационный файл
settings.ktae.xml	Конфигурационный файл

kaspersky

Установка Kaspersky Threat Attribution Engine

В этой главе представлена информация об установке программы Kaspersky Threat Attribution Engine.

В этой главе

О процессе установки

В этом разделе описывается процесс установки и среда.

О компонентах Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine состоит из следующих компонентов:

- Служба Kaspersky Threat Attribution Engine

  Это основная служба, обеспечивающая всю функциональность Kaspersky Threat Attribution Engine.
- Служба обновления

  Эта служба скачивает обновления баз Kaspersky Threat Attribution Engine.

О периметрах

Kaspersky Threat Attribution Engine необходимо установить в двух средах:

- Открытый периметр

  Эта среда имеет доступ в Интернет. В этой среде установлена служба Updater.
- Безопасный периметр

  Это безопасная среда. Обычно эта среда отделена от открытого периметра прослойкой. В этой среде установлена служба Kaspersky Threat Attribution Engine.

  > Инструкции по установке в следующих разделах предлагают два подхода. Первый - когда ваш защищенный периметр имеет доступ к Интернету, второй - когда доступ к Интернету отсутствует.

О процессе установки

Процесс установки состоит из двух этапов:

kaspersky

1. Этап 1. Установка службы Updater в открытый периметр (см. раздел «Этап 1. Установка службы обновления» на стр.12).
2. Этап 2. Установка службы Kaspersky Threat Attribution Engine в защищенный периметр (см. раздел «Этап 2. Установка службы Kaspersky Threat Attribution Engine» на стр. 12).

Этап 1. Установка службы обновления

На этом этапе установите службу Updater в открытый периметр.

► *Чтобы установить службу Updater:*

1. Запустите скрипт install_ktae_updater.sh:

   ```
   bash install_ktae_updater.sh
   ```

2. Введите значение `2` и нажмите ENTER.

   Выбрана опция *Установить программу обновления KTAE*.

3. Прочтите и примите Лицензионное соглашение с конечным пользователем (EULA):
   - Введите значение `Y` и нажмите ENTER, чтобы принять лицензионное соглашение.
   - Введите значение `N` и нажмите ENTER, чтобы отклонить лицензионное соглашение.

     Процесс установки завершен.
4. Дождитесь завершения установки.
5. Измените текущую рабочую директорию на / opt / ktae-updater:

   ```
   cd / opt / ktae-updater
   ```

6. Загрузите обновления Kaspersky Threat Attribution Engine, выполнив следующую команду:

   ```
   bash download_all.sh% updates_folder%
   ```

   В приведенной выше команде замените `% updates_folder%` на путь к директории, в которой будут храниться файлы обновлений.

   Не пропускайте шаг 5. Файлы обновления необходимы для установки Kaspersky Threat Attribution Engine.

Этап 2. Установка службы Kaspersky Threat Attribution Engine

На этом этапе установите службу Kaspersky Threat Attribution Engine в защищенный периметр.

Этот этап состоит из следующих фаз:

- Фаза 1. Установите зависимости и настройте MySQL.
- Фаза 2. Запустите установочный скрипт.
- Фаза 3. Измените пароль по умолчанию для ktae_user в MySQL.

- Фаза 4. Укажите контрольную фразу сертификата.
- Фаза 5. Запустите службу Kaspersky Threat Attribution Engine.
- Фаза 6. Импортируйте базы данных в MySQL.
- Фаза 7. Добавьте директории для загруженных и извлеченных файлов в исключения брандмауэра.
- Фаза 8. Настройте обновления и обновите Kaspersky Threat Attribution Engine.
- Фаза 9. Откройте веб-интерфейс и добавьте сертификат в список доверенных сертификатов.

Ниже приведены инструкции по фазам.

Фаза 1. Установите зависимости и настройте MySQL

► *Если у вашего защищенного периметра есть доступ к Интернету:*

1. Не устанавливайте зависимости вручную.
2. Выполните скрипт, устанавливающий зависимости:

   ```
   bash 00_install_dependencies.sh
   ```
3. Измените пароль root MySQL
4. Введите значение `y` и нажмите ENTER для всех вопросов безопасности MySQL.

► *Если у вашего защищенного периметра нет доступа к Интернету:*

1. Установите все зависимости вручную (см. раздел «Аппаратные и программные требования» на стр. 5).

   Некоторые из необходимых зависимостей входят в комплект поставки.
2. Остановите службу MySQL:

   ```
   systemctl остановить mysqld
   ```
3. Добавьте параметр `local_infile = 1` в файл /etc/my.conf:

```
[mysqld]
local_infile = 1
```

4. Убедитесь, что владельцем файла /etc/my.conf является `mysql: mysql`.

   Например, для этого вы можете использовать команду `ls -l /etc/my.conf`.
5. Загрузите другие рекомендуемые настройки из файла conf / my.conf дистрибутива в файл /etc/my.conf:

```
[mysqld]
bind-address = 0.0.0.0
port = 3306
disable_log_bin
key_buffer_size=32M
default-storage-engine=innodb
innodb_buffer_pool_size=512M
innodb_buffer_pool_instances=8
innodb_log_buffer_size=8M
innodb_write_io_threads=64
innodb_read_io_threads=64
innodb_parallel_read_threads=64
innodb_io_capacity=100000
innodb_change_buffer_max_size=50
innodb_compression_level=9
innodb_log_file_size=32M
innodb_file_per_table
innodb_flush_log_at_trx_commit=0
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

6. Запустите службу MySQL:

   ```
   systemctl start mysqld
   ```

Фаза 2. Запустите установочный скрипт

► *В этой фазе:*

1. Выполните сценарий 01_install_ktae.sh:

   ```
   bash 01_install_ktae.sh
   ```

2. Убедитесь, что все зависимости установлены.
3. Убедитесь, что токен доступен. В списке USB-устройств должно отображаться следующее: `0529:0620 Alladin`.
4. Введите значение `1` и нажмите ENTER.

   Выбрана опция *Установить службу KTAE*.
5. Прочтите и примите Лицензионное соглашение с конечным пользователем (EULA):
   - Введите значение `Y` и нажмите ENTER, чтобы принять лицензионное соглашение.
   - Введите значение `N` и `нажмите` ENTER, чтобы отклонить лицензионное соглашение.

     Процесс установки завершен.
6. Введите парольную фразу несколько раз, чтобы сгенерировать самозаверенный сертификат SSL.

   Держите парольную фразу под рукой, чтобы вы могли указать ее позже в файле конфигурации Kaspersky Threat Attribution Engine.

Рекомендуем использовать собственный сертификат (см. раздел «Работа с сертификатами» на стр. 63).

7. Введите пароль root MySQL для схемы базы данных Kaspersky Threat Attribution Engine и SQL-скрипта, создающего пользователей.
8. Убедитесь, что служба MySQL запущена. Должен отображаться `активный (рабочий)` статус.
9. Отображается список директорий. Убедитесь, что следующие директории присутствуют и имеют `ktae: ktae` в качестве владельца:
   - /opt/ktae
   - /opt/ktae/uploaded
   - /opt/ktae/extracted
10. Убедитесь, что утилиты `генотип` и `строки` имеют права на выполнение:
    - /opt/ktae/tools/linux/genotype
    - /opt/ktae/tools/linux/binutils/strings
11. Убедитесь, что у пользователя `ktae` есть разрешение на чтение для доступа к сгенерированному сертификату (/opt/ktae/cert/server.p12).

    В качестве альтернативы замените сгенерированный сертификат вашим собственным сертификатом.

Фаза 3. Измените пароль по умолчанию для ktae_user в MySQL

► *В этой фазе:*

1. Выполните следующую команду:

   ```
   mysql -u ktae_user -p;
   ```
2. Введите пароль по умолчанию:

   ```
   kcxB8L {Qm [{VX% 5U
   ```
3. Измените пароль с помощью следующей команды:

   ```
   set password = '%new_password%';
   ```

   В приведенной выше команде замените `%new_password%` новым надежным паролем.

   Для баз данных MySQL, чтобы соответствовать минимальным условиям, необходимым для надежного пароля, пароль должен содержать как минимум:
   - Девять персонажей
   - Две заглавные буквы
   - Две строчные буквы
   - Два числа
   - Два из следующих допустимых специальных символов: `'` , `~` , `!` , `@`, `#`, `$`, `%`, `^`, `&`, `*`, `(`, `)`, `_`, `-`, `+`, `=`, `{`, `}`, `[`, `]`, `/`, `<`, `>`, `,` , `.` , `;` , `?` , `'` ,: , `|` , и пробел.
4. Выйдите из клиента MySQL:

   ```
   quit;
   ```

5. Укажите новый пароль в файле /opt/ktae/conf/application.conf, в разделе database> mysql> properties> password:

```
database {
  mysql {
    properties = {
      url =
"jdbc:mysql://"${database.mysql.properties.serverName}":"${database.mysql
.properties.portNumber}"/"${database.mysql.properties.databaseName}"?allo
wLocalInfile=true&rewriteBatchedStatements=true&allowPublicKeyRetrieval=t
rue"
      serverName = "localhost"
      portNumber = "3306"
      user = "ktae_user"
      password = "%new_password%" // <-- введите ваш новый пароль здесь
      databaseName="ktae"
    }
  }
...
}
```

Фаза 4. Укажите парольную фразу сертификата

► *В этой фазе:*

1. Укажите парольную фразу из фазы 1 в файле /opt/ktae/conf/application.conf в разделе service-settings> tls-settings> key-store-password:

```
service-settings {
  host = "0.0.0.0"
  port = 8080

  tls-settings {
    key-store-path = "/opt/ktae/cert/server.p12"
    key-store-password = "%password%" // <-- введите вашу новую парольную
фразу для сертификата здесь
  }
...
}
```

Если вы используете собственный сертификат (см. раздел «Работа с сертификатами» на стр. 63), укажите для него парольную фразу.

5 этап. Запустите сервис Kaspersky Threat Attribution Engine.

► *На этом этапе:*

1. Запустите сценарий 02_run_ktae.sh:

```
bash 02_run_ktae.sh
```

Появится список статусов услуг.

2. Убедитесь, что служба kavehost находится в *рабочем* состоянии.

3. Убедитесь, что служба `ktae` находится в *рабочем* состоянии.
4. Проверьте файл журнала Kaspersky Threat Attribution Engine (logs / logFile.txt) на наличие ошибок.

Фаза 6. Импортировать базы данных в MySQL

► *В этой фазе:*

1. Выполните сценарий 03_discard_db_tables.sh, чтобы подготовить базу данных для импорта данных:

   ```
   bash 03_discard_db_tables.sh
   ```

2. Введите пароль пользователя root MySQL.
3. Выполните сценарий 04_copy_db_tables.sh:

   ```
   bash 04_copy_db_tables.sh
   ```

4. Введите путь к файлам, содержащим данные базы данных
5. Сравните хеши MD5 файлов информации базы данных с хешами MD5 из файла txt / ktae_data_md5s.txt. Хеши должны быть идентичными.
6. Выполните сценарий 05_import_db_tables.sh:

   ```
   bash 05_import_db_tables.sh
   ```

Фаза 7. Добавьте директории для загруженных и извлеченных файлов в исключения брандмауэра

► *В этой фазе:*

1. Убедитесь, что в исключения антивируса добавлены следующие директории:
   - /opt/ktae/uploaded
   - /opt/ktae/extracted
   - /opt/ktae/share

Фаза 8. Настроить обновления и обновить Kaspersky Threat Attribution Engine.

► *В этой фазе:*

1. Укажите директорию, в которой Kaspersky Threat Attribution Engine будет искать файлы обновлений. Эта директория указана в /opt/ktae/conf/application.conf, в разделе database > updates >:

```
database {
...
  updates {
    path = "/opt/ktae/updates_path" // <-- specify your update directory
here
    Пользовательскиеer-id = "example_Пользовательскиеer_id"
  }
}
```

2. Убедитесь, что указанная директория обновлений присутствует и имеет `ktae: ktae` в качестве его владельца.
3. Сохраните загруженные файлы обновлений на Этапе 1. Установка службы обновления (см. стр. 12) в указанную директорию обновления.

4. Запустите утилиту admin_cli:

   ```
   bash / opt / ktae / bin / admin_cli
   ```

5. Остановите службу, запустив команду `ts`.
6. Обновите базы данных DeepUnpack, выполнив команду `duu`.
7. Запустите службу, выполнив команду `rs`.

Фаза 9. Откройте веб-интерфейс и добавьте сертификат в список доверенных сертификатов.

► *В этой фазе:*

1. В браузере перейдите по адресу https: // localhost: 8080.
2. Добавьте сгенерированный сертификат SSL в исключения браузера.

   Если вы используете свой собственный сертификат, возможно, вам также придется выполнить этот шаг.

kaspersky

Руководство пользователя

В этой главе содержится информация об использовании программы Kaspersky Threat Attribution Engine для анализа и атрибуции угроз.

В этой главе

Руководство по веб-интерфейсу

В этом разделе описывается веб-интерфейс программы Kaspersky Threat Attribution Engine.

В этом разделе

kaspersky

Страница авторизации

Страница входа используется для входа в Kaspersky Threat Attribution Engine.

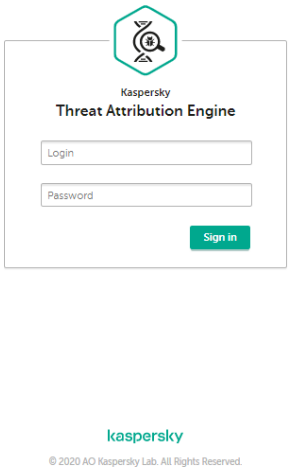

Рисунок 2: Страница авторизации

► *Чтобы перейти на эту страницу:*

1. В браузере перейдите по адресу `https: // localhost: 8080`.
2. Откроется страница **Вход в систему**.

Элементы страницы:

- **Логин**. Логин пользователя.
- **Пароль**. Пользовательский пароль.
- **Авторизуйтесь**. Войдите в Kaspersky Threat Attribution Engine, используя указанные имя пользователя и пароль.

Действия для этой страницы: Вход в Kaspersky Threat Attribution Engine (см. стр. 40).

Главное меню

Главное меню позволяет перемещаться между страницами веб-интерфейса.

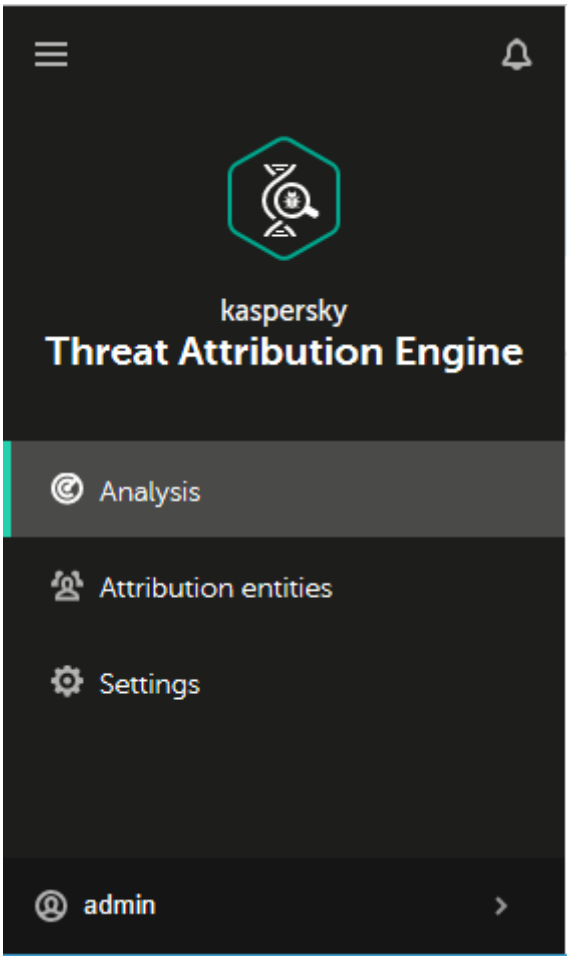

Рисунок 3: Главное меню

Главное меню включает следующие элементы:

- **Свернуть**. Сворачивает меню (этот элемент находится в верхнем левом углу экрана). Нажмите на эту кнопку еще раз, чтобы раскрыть меню.
- **Анализ**. Открывает страницу анализа (см. раздел «Страница анализа» на стр. 22).
- **Объекты атрибуции**. Открывает страницу объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).
- **Настройки**. Открывает страницу настроек (см. раздел «Страница настроек» на стр. 38).
- **Имя пользователя**. Отображает имя текущего пользователя.
- **Выйти**. Появляется, когда пользователь наводит курсор на параметр **Администратор**. Элемент **Выйти** завершает текущий сеанс и возвращает пользователя к странице **входа в систему** (см. раздел «Страница входа » на стр. 20).
- **Уведомления**. Отображает уведомления (этот элемент расположен в правом верхнем углу экрана).

kaspersky

Страница анализа

На странице анализа отображаются результаты недавнего анализа файлов. На этой странице можно выполнить новый анализ файлов.

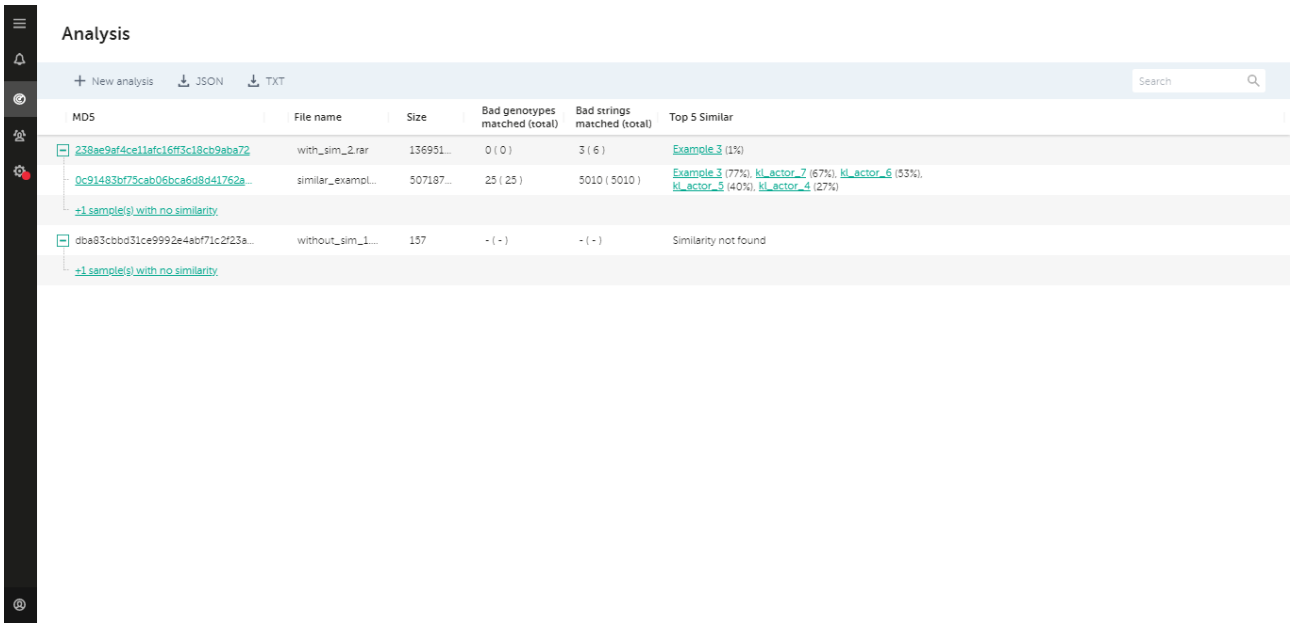

Рисунок 4: Страница анализа

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21), выберите **Анализ**.
2. Откроется страница анализа.

На этой странице присутствуют следующие элементы:

- **Новый анализ**. Открывает новую страницу анализа.
- **JSON**. Скачивает отчет в формате JSON.
- **TXT**. Скачивает отчет в формате TXT.
- **Искать**. Фильтрует содержимое таблицы по указанной строке поиска.
- **Отменить**. Если анализ еще не завершен, вы можете отменить его на этой странице. Анализ всех файлов, которые еще не были проанализированы, будет отменен. В таблице результатов анализа будут отображаться результаты для файлов, которые были проанализированы, в то время как для всех других файлов будет отображаться статус отмененного анализа.
- Таблица результатов анализа. Отображает результаты анализа для всех проанализированных файлов.

На этой странице доступны следующие действия:

- Отправка файлов на анализ и атрибуцию (см. стр. 41).
- Интерпретация результатов анализа (см. стр. 42).
- Скачивание отчетов (см. стр. 49).

Результаты анализа

Отдельные результаты анализа могут иметь вложенные записи, если образец, отправленный на анализ, был распакован. В этом случае будут показаны только те записи, которые соответствуют известным объектам атрибуции. Все остальные записи будут свернуты.

В результатах анализа отображается следующая информация:

- **MD5**. MD5-хеш анализируемого файла.

  Нажатие на элемент в столбце **MD5** на странице анализа открывает страницу результатов анализа (см. раздел «Страница результатов анализа» на стр. 25).

  Если этот элемент не является ссылкой, то в этом образце нет связанных деталей анализа.

- **Имя файла**. Имя анализируемого файла.
- **Размер**. Размер файла в байтах.
- **Совпадение неправильных генотипов (всего)**. Количество генотипов в анализируемой выборке, совпадающих с генотипами в образцах, аналогичных этому образцу. Число в скобках - это общее количество генотипов в проанализированной выборке, которые совпали с выборками известных объектов атрибуции.
- **Совпадение неверных строк (всего)**. Количество строк в анализируемой выборке, совпадающих со строками в выборках, аналогичных этой выборке. Число в скобках - это общее количество неверных строк в проанализированной выборке, которые совпадают с выборками известных объектов атрибуции.
- **Топ-5 похожих**. Пять основных объектов атрибуции, у которых есть образцы, наиболее похожие на анализируемые.

  Независимо от того, разрешен ли образец или были ошибки во время анализа, в этом поле отображается статус.

  При нажатии на имя объекта атрибуции в этом элементе открывается страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).

  В этом поле также отображаются другие статусы, если сходства с объектами атрибуции не обнаружено. Для получения дополнительной информации см. «Интерпретация результатов анализа» на стр. 42.

kaspersky

Страница нового анализа

В окне **Новый анализ**, доступном со страницы **Анализ**, вы можете отправлять файлы на анализ.

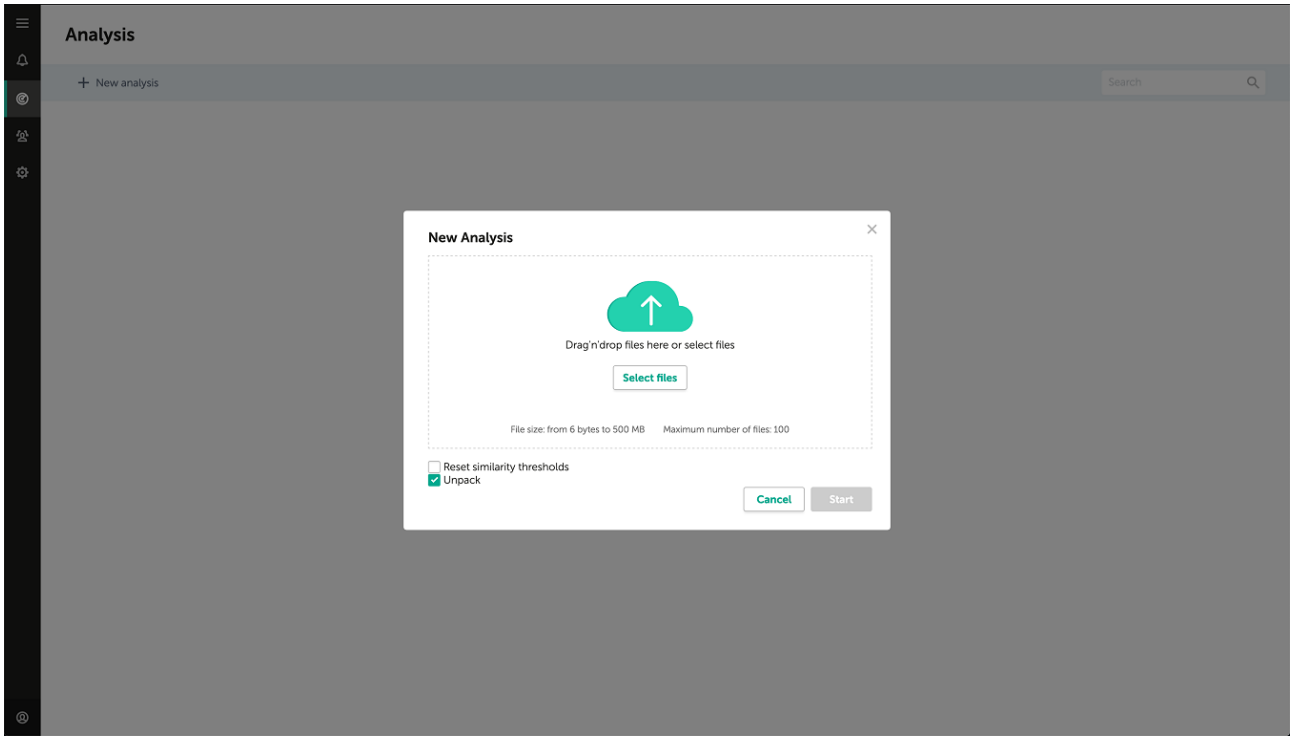

Рисунок 5: Новое окно анализа

► *Чтобы перейти к этому окну:*

1. В главном меню (см. стр. 21), выберите **Анализ**.
2. На этой странице (см. раздел «Страница анализа» на стр. 22) нажмите на кнопку **Новый анализ**.
3. Откроется окно **Новый анализ**.

Это окно содержит следующие элементы:

- **Перетащить файлы**. Перетащите файлы мышью в эту зону, чтобы отправить их на анализ.
- **Выбрать**. Открывает окно браузера, в котором вы можете выбрать файлы для анализа.
- **Сбросить пределы схожести**. Игнорирует пределы схожести для сравниваемых образцов.
- **Распаковать**. Указывает, что содержимое прикрепленных файлов необходимо распаковать для анализа.
- **Старт**. Отправляет файлы на анализ.
- **Отменить**. Возврат на страницу анализа (см. раздел «Страница анализа» на стр. 22).

На этой странице доступны следующие действия: отправка файлов на анализ и атрибуцию (см. стр. 41).

Страница результатов анализа

На странице результатов анализа отображается информация о проанализированном образце.

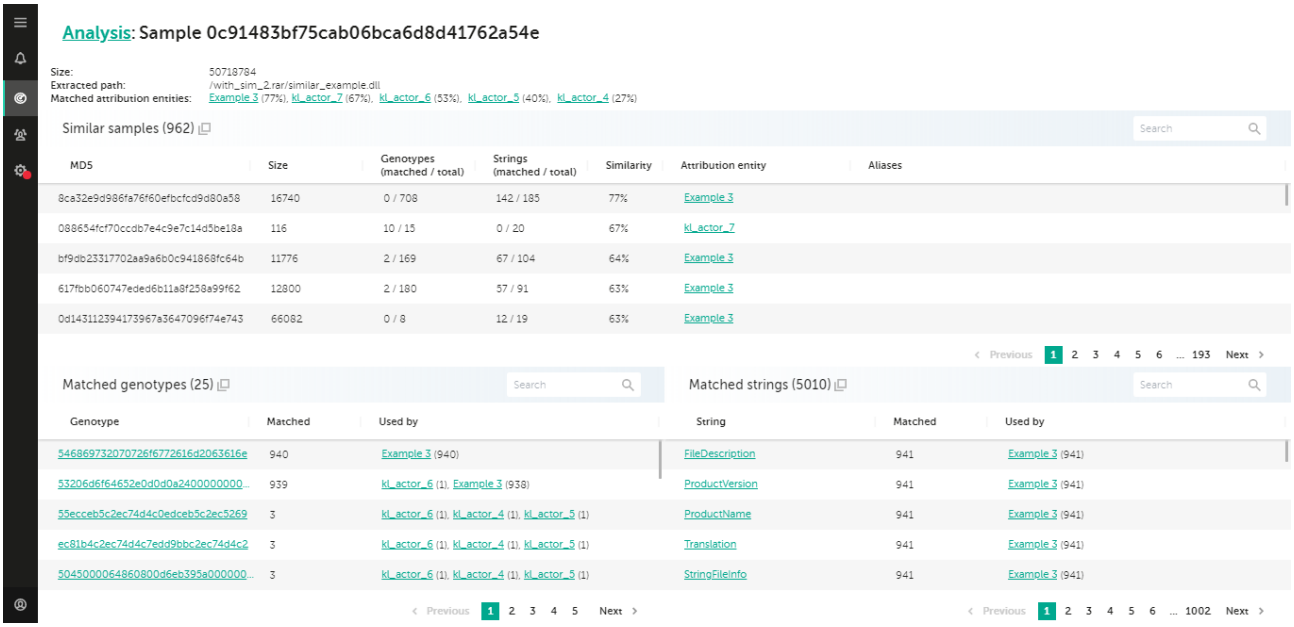

Рисунок 6: Страница результатов анализа

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21), выберите **Анализ.**
2. На этой странице (см. раздел «Страница анализа» на стр. 22) нажмите на анализируемый образец в столбце **MD5**.
3. Откроется страница результатов анализа.

Вы делаете выбор на странице. Нажав на **Анализ** в верхней части экрана, вы вернетесь на страницу анализа.

Страница результатов анализа содержит следующие разделы:

- Главная информация. Эта область вверху страницы содержит общую информацию об анализируемом образце.
- **Похожие образцы**. Содержит информацию об аналогичных образцах.
- **Совпадающие генотипы**. Содержит информацию о генотипах в анализируемом образце, которые совпадают с генотипами в образцах, аналогичных этому образцу.
- **Совпадающие строки**. Содержит информацию о строках в проанализированном образце, которые совпадают со строками в образцах, аналогичных этому образцу.

Страница результатов анализа содержит следующие элементы:

- **Искать**. Выполняет поиск хешей MD5, объектов атрибуции, алиасов, генотипов и строк в связанной таблице.

На этой странице доступны следующие действия: интерпретация результатов анализа (см. стр. 42).

Главная информация

Эта область вверху страницы содержит данные об анализируемом образце:

- **Размер**. Размер анализируемой выборки в байтах.
- **Путь извлечения**. Путь в родительском образце к текущему образцу. Используется для образцов, распакованных для анализа.
- **Соответствующие объекты атрибуции**. Список объектов атрибуции, соответствующих этому образцу.

  Если указанный процент рядом с именем объекта атрибуции равен 100%, то этот объект атрибуции владеет этим образцом. Это означает, что этот объект атрибуции является единственным объектом атрибуции, относящимся к данной выборке.

  При нажатии на объект атрибуции открывается страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).

Похожие образцы

В этом разделе отображается информация об аналогичных образцах:

- **MD5**. MD5-хеш аналогичного образца.
- **Размер**. Размер файла образца.
- **Генотипы (совпадающие / всего)**. Количество генотипов в подобной выборке, которые соответствуют текущей выборке, за которым следует общее количество генотипов в аналогичной выборке, связанных с объектом атрибуции.
- **Строки (совпадающие / всего)**. Количество строк в аналогичной выборке, соответствующих текущей выборке, за которым следует общее количество строк в аналогичной выборке, связанных с объектом атрибуции.
- **Сходство**. Процент сходства между анализируемым образцом и аналогичным образцом.
- **Сущность атрибуции**. Сущность атрибуции, которой принадлежит этот образец.

  При нажатии на имя объекта атрибуции открывается страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).
- **Алиасы**. Известные алиасы объекта атрибуции, которому принадлежит этот образец.

Соответствующие генотипы

В этом разделе отображается информация о генотипах в выборке, которые были сопоставлены с генотипами аналогичных выборок:

- **Генотип**. Генотип в образце, который соответствовал генотипам аналогичных образцов.

  При нажатии на идентификатор генотипа открывается страница свойств генотипа (см. раздел «Страница свойств генотипа» на стр. 27).
- **Соответствие**. Количество известных образцов объектов атрибуции, имеющих этот генотип.
- **Использование**. Сущности атрибуции, владеющие образцами с этим генотипом. Число в круглых скобках указывает, сколько образцов объекта атрибуции имеют этот генотип.

Соответствующие строки

В этом разделе отображается информация о строках в образце, которые были сопоставлены строкам из аналогичных образцов:

- **Строка**. Строка в образце, сопоставленная со строками аналогичных образцов.

  При нажатии на строковой идентификатор открывается страница свойств строки. (см. раздел «Страница свойств строки» на стр. 28).
- **Соответствие**. Количество известных образцов сущностей атрибуции, имеющих эту строку.
- **Использование**. Сущности атрибуции, которым принадлежат образцы с этой строкой. Число в скобках указывает, сколько образцов объекта атрибуции имеют эту строку.

Страница свойств генотипа

На странице свойств генотипа отображается информация о генотипе.

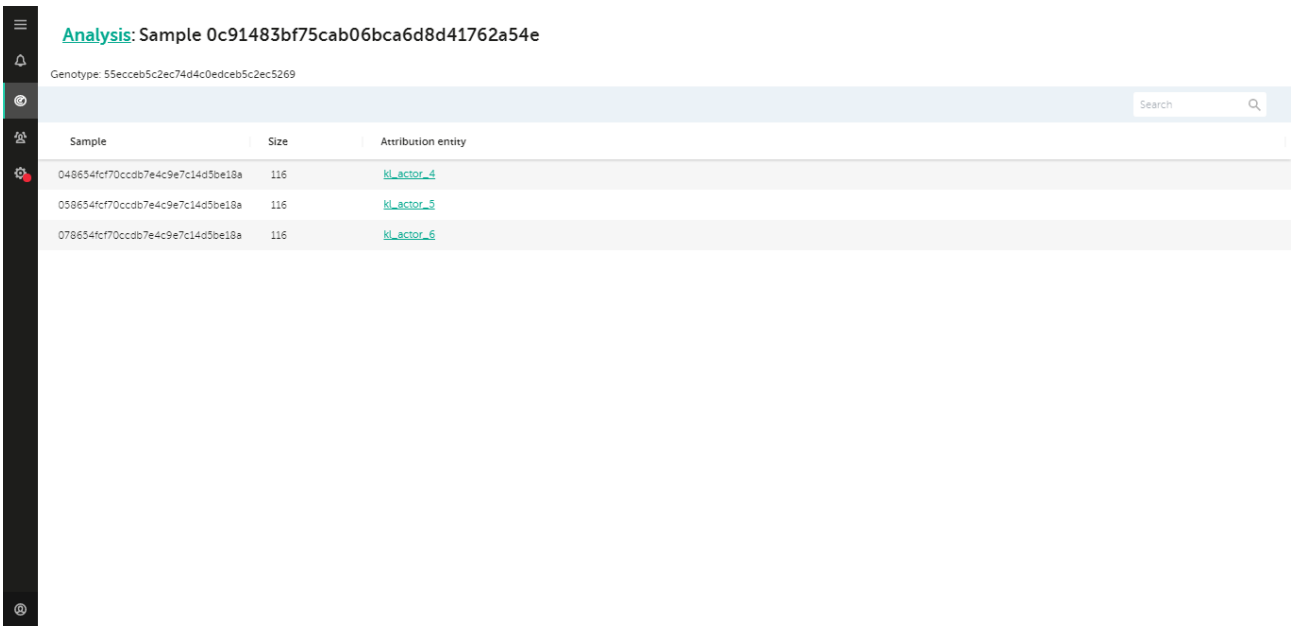

Рисунок 7: Страница свойств генотипа

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21), выберите **Анализ**.
2. На этой странице (см. раздел «Страница анализа» на стр. 22) нажмите на анализируемый образец в столбце **MD5**.

   Откроется страница результатов анализа (см. раздел «Страница результатов анализа» на стр. 25).
3. На странице результатов анализа (см. раздел «Страница результатов анализа » на стр.25) нажмите на выбранный генотип.
4. Откроется страница свойств генотипа.

Страница свойств генотипа содержит следующие элементы:

- **Анализ**. Открывает страницу результатов анализа (см. раздел «Страница результатов анализа» на стр. 25) страница.
- **Искать**. Ищет генотип в таблице образцов.

- **Данные генотипа**. Таблица, отображающая данные о генотипе.

На этой странице доступны следующие действия: интерпретация результатов анализа (см. стр. 42).

Данные генотипа

В этой таблице отображается информация о генотипе:

- **Образец**. Пример объекта атрибуции с этим генотипом.
- **Размер**. Размер файла образца в байтах.
- **Сущность атрибуции**. Сущность атрибуции, которой принадлежит образец.

  При нажатии на имя объекта атрибуции открывается страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).

Страница свойств строки

На странице свойств строки отображается информация о строке.

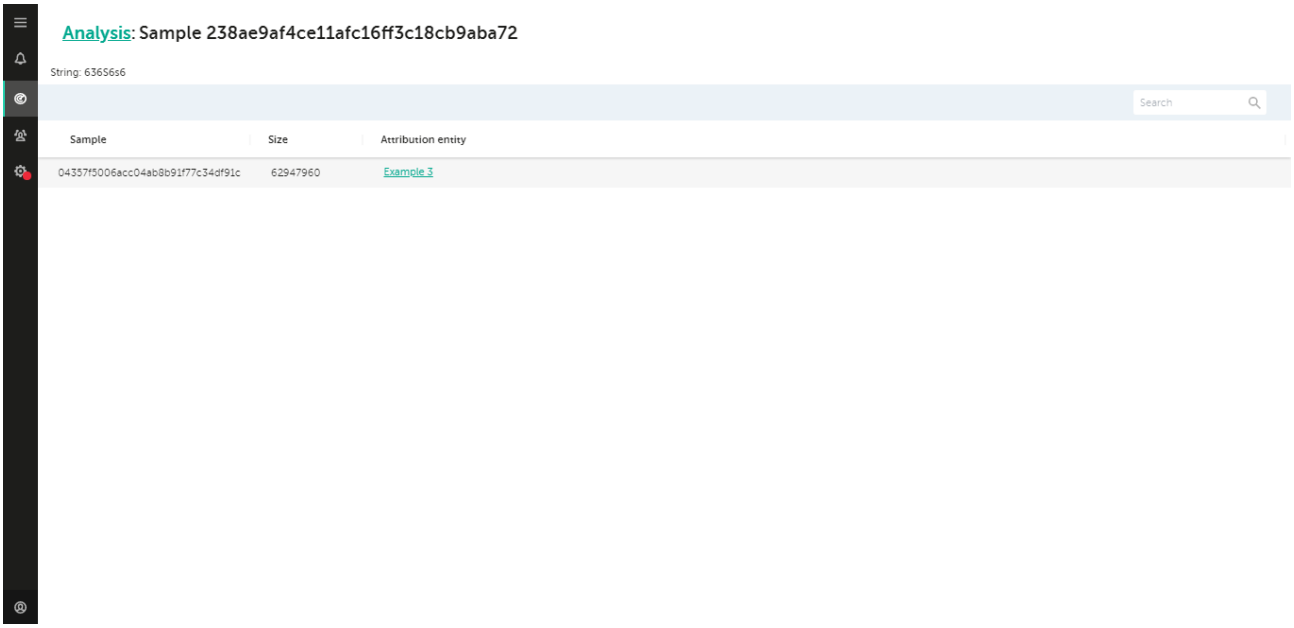

Рисунок 8: Страница свойств строки

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21), выберите **Анализ**.
2. На этой странице (см. раздел «Страница анализа» на стр. 22) Нажмите на анализируемый образец в столбце **MD5**.

   Откроется страница результатов анализа (см. раздел «Страница результатов анализа» на стр. 25).
3. На странице результатов анализа (см. раздел «Страница результатов анализа» на стр. 25) нажмите на выбранную строку.
4. Откроется страница свойств строки.

Страница свойств строки содержит следующие элементы:

- **Анализ**. Возврат к странице результатов анализа (см. раздел «Страница результатов анализа» на стр. 25).
- **Искать**. Ищет строку в таблице образцов.
- **Данные строки**. Таблица с данными о строке.

На этой странице доступны следующие действия: интерпретация результатов анализа (см. стр. 42).

Данные строки

В этой таблице отображается информация о строке:

- **Образец**. Образец объекта атрибуции с этой строкой.
- **Размер**. Размер файла образца в байтах.
- **Сущность атрибуции**. Сущность атрибуции, которой принадлежит образец.

  При нажатии на имя объекта атрибуции открывается страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).

Страница объектов атрибуции

На странице **Объекты атрибуции** отображается список объектов атрибуции, известных Kaspersky Threat Attribution Engine, и вы можете управлять объектами атрибуции и соответствующими образцами.

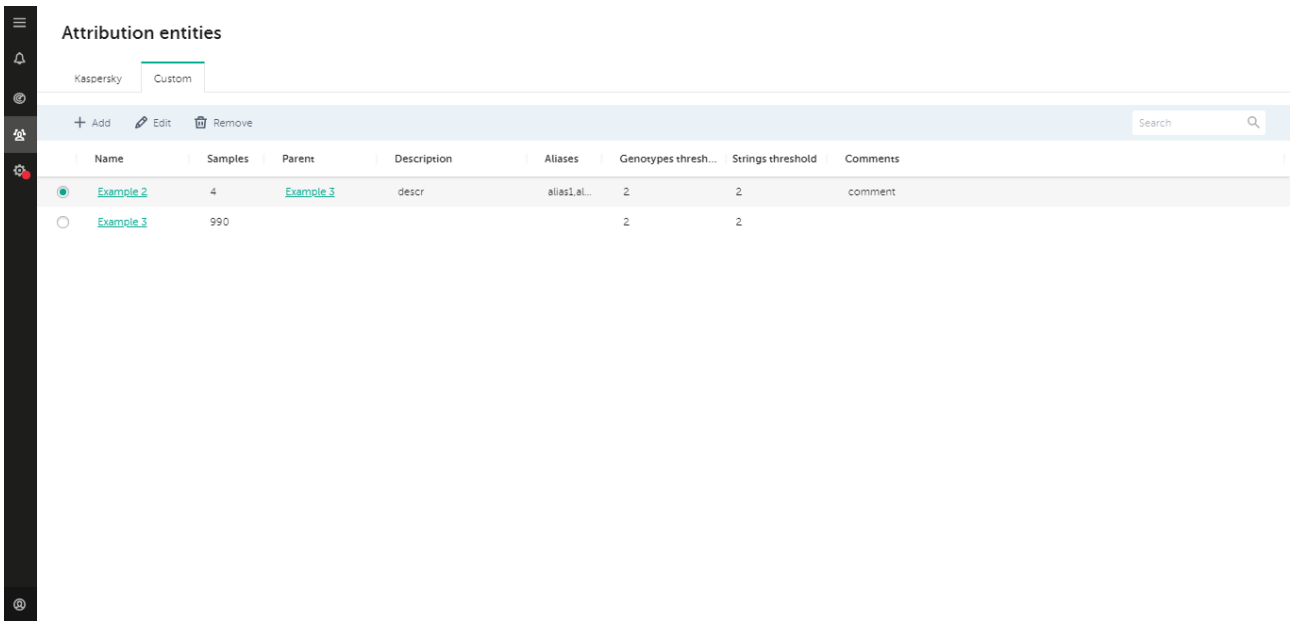

Рисунок 9: Страница объектов атрибуции

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).

На этой странице есть две вкладки:

- **Kaspersky**. Информация об объектах атрибуции, предоставленная «Лабораторией Касперского».

- **Пользовательские**. Информация о пользовательских объектах атрибуции.

Элементы вкладки **Kaspersky**:

- **Сущности атрибуции**. Таблица атрибутов сущностей с расширенной информацией о них. Вы можете выбрать объект атрибуции для выполнения операций с ним.
- **Искать**. Фильтрует содержимое таблицы по указанной строке поиска.

Элементы вкладки **Пользовательские**:

- **Сущности атрибуции**. Таблица атрибутов сущностей с расширенной информацией о них. Вы можете выбрать объект атрибуции для выполнения операций с ним.
- **Добавить**. Открывает страницу новой сущности атрибуции (см. раздел «Страница новой сущности атрибуции» на стр. 31). Объект атрибуции не может быть выбран в списке объектов атрибуции, чтобы эта опция была доступна.
- **Редактировать**. Открывает страницу свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).
- **Удалить**. Удаляет текущий выбранный объект атрибуции (с подтверждением).
- **Искать**. Фильтрует содержимое таблицы по указанной строке поиска.

На этой странице доступны следующие действия:

- Управление объектами атрибуции (см. стр. 45).
- Управление файлами, связанными с объектами атрибуции (см. раздел «Управление образцами, связанными с объектами атрибуции» на стр. 47).

Сущности атрибуции

Таблица объектов атрибуции отображает следующую информацию об объектах атрибуции:

- **Маркер выделения**. Нажатие на этот маркер выбирает объект атрибуции.
- **Имя**. Имя объекта атрибуции. При нажатии на имя открывается страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).
- **Образцы**. Количество образцов, принадлежащих этому объекту атрибуции.

  Если выполняется операция прикрепления образца, вместо количества образцов отображается ссылка «прикрепление». Вы можете нажать на эту ссылку, чтобы перейти к образцу журнала вложений в свойствах объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).
- **Родительская сущность**. Сущность атрибуции, которая является родительской для текущей сущности атрибуции. При нажатии на имя объекта атрибуции открывается страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).
- **Описание**. Описание объекта атрибуции.
- **Алиасы**. Список известных алиасов для этого объекта атрибуции.
- **Предел генотипов**. Минимальное количество генотипов, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Если в выборке больше совпадающих генотипов, чем указанное число, эта сущность атрибуции отображается как аналогичная сущность атрибуции в выборке.
- **Предел строк**. Минимальное количество строк, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Если в выборке найдено больше совпадающих строк, чем

указанное число, эта сущность атрибуции отображается как аналогичная сущность атрибуции в выборке.

- **Комментарии**. Дополнительная информация о сущности атрибуции.

Страница новой атрибуции

Вы можете использовать страницу «Новая сущность атрибуции» для добавления новых пользовательских сущностей атрибуции.

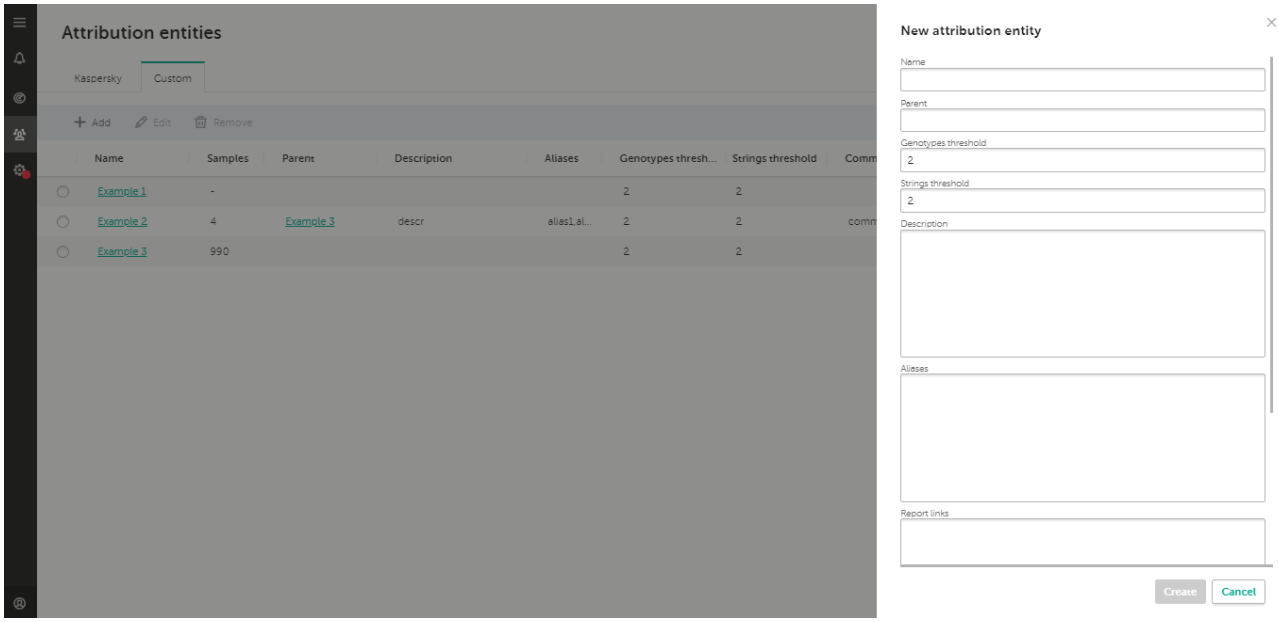

Рисунок 10: Страница новой атрибуции

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр.29).
2. Выберите вкладку **Пользовательские**.
3. Нажмите на кнопку **Добавить**.
4. Откроется страница нового объекта атрибуции.

Элементы страницы:

- **Имя**. Имя объекта атрибуции.
- **Родительский объект**. Имя родительского объекта атрибуции.
- **Предел генотипов**. Минимальное количество генотипов, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Если в выборке больше совпадающих генотипов, чем указанное число, эта сущность атрибуции отображается как аналогичная сущность атрибуции в выборке.
- **Предел строк**. Минимальное количество генотипов, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Если в выборке больше совпадающих генотипов, чем

указанное число, эта сущность атрибуции отображается как аналогичная сущность атрибуции в выборке.

- **Описание**. Описание объекта атрибуции.
- **Алиасы**. Список известных алиасов для этого объекта атрибуции.
- **Ссылки на отчеты**. Ссылки на отчеты, связанные с этим объектом атрибуции.
- **Комментарии**. Дополнительная информация о сущности атрибуции.
- **Создать**. Добавляет объект атрибуции в список объектов атрибуции.
- **Отменить**. Отменяет указанную информацию и открывает страницу объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр.29).

На этой странице доступны следующие действия: управление объектами атрибуции (см. стр. 45).

Страница обновления объекта атрибуции

Вы можете использовать страницу «Обновить объект атрибуции» для редактирования свойств объекта атрибуции.

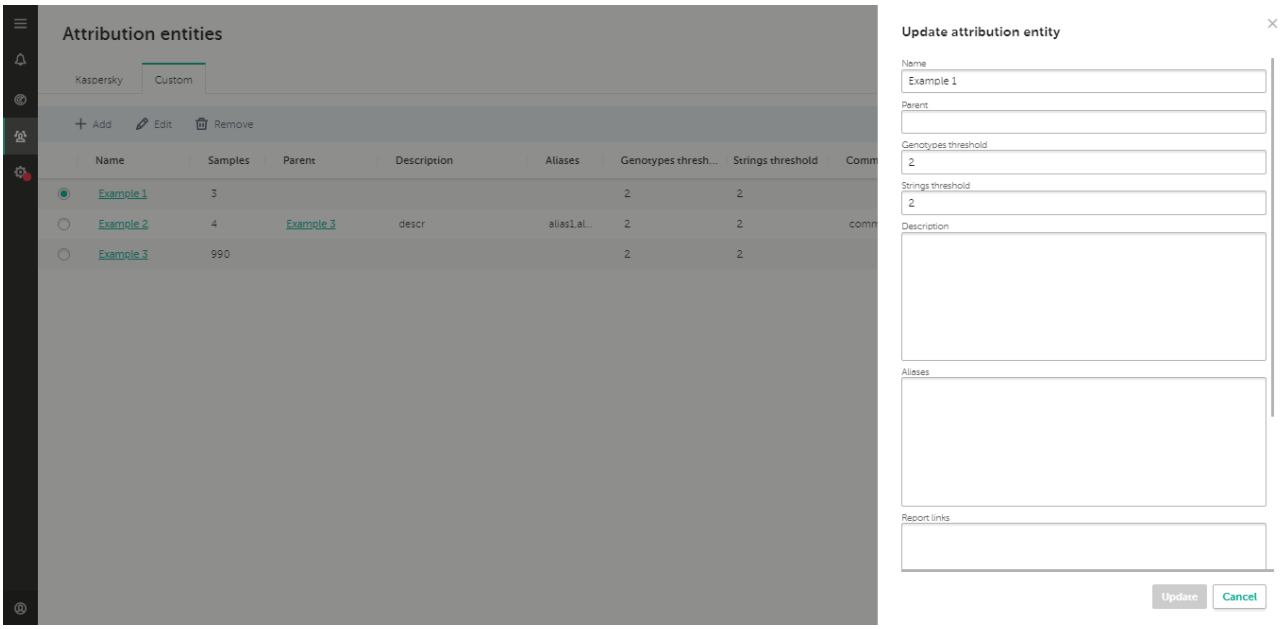

Рисунок 11: Обновить страницу объекта атрибуции

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр.29).
2. Выберите вкладку **Пользовательские**.
3. Нажмите на кнопку **Редактировать**.
4. Откроется страница **Обновить объект атрибуции**.

Элементы страницы:

- **Имя**. Имя объекта атрибуции.
- **Родительский объект**. Имя родительского объекта атрибуции.
- **Предел генотипов**. Минимальное количество генотипов, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Если в выборке больше совпадающих генотипов, чем указанное число, эта сущность атрибуции отображается как аналогичная сущность атрибуции в выборке.
- **Предел строк**. Минимальное количество генотипов, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Если в выборке больше совпадающих генотипов, чем указанное число, эта сущность атрибуции отображается как аналогичная сущность атрибуции в выборке.
- **Описание**. Описание объекта атрибуции.
- **Алиасы**. Список известных алиасов для этого объекта атрибуции.
- **Ссылки на отчеты**. Ссылки на отчеты, связанные с этим объектом атрибуции.
- **Комментарии**. Дополнительная информация о сущности атрибуции.
- **Обновить**. Обновляет свойства объекта атрибуции.
- **Отменить**. Отменяет указанную информацию и открывает страницу объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр.29).

На этой странице доступны следующие действия: управление объектами атрибуции (см. стр. 45).

Страница прикрепления образцов

На странице прикрепления образцов вы можете прикрепить образцы для существующего объекта атрибуции.

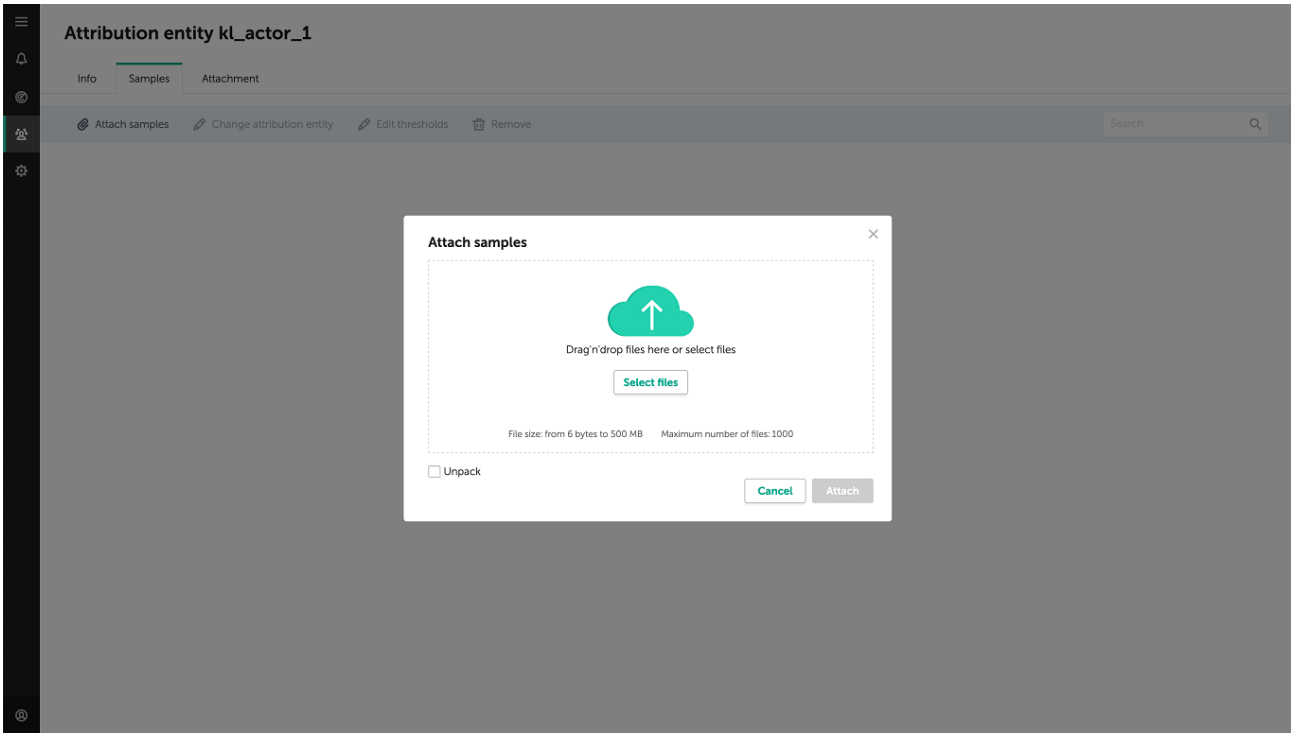

Рисунок 12: Прикрепите страницу с образцами

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).

2. Нажмите на имя объекта атрибуции.

   Откроется страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).

3. Выберите вкладку **Образцы**.
4. Нажмите на кнопку **Прикрепить образцы**.
5. Откроется окно **Прикрепить образцы**.

Это окно содержит следующие элементы:

- **Перетащить файлы**. Перетащите файлы мышью в эту зону, чтобы прикрепить их к объекту атрибуции.
- **Выбрать**. Открывает окно браузера, в котором вы можете выбрать файлы для прикрепления.
- **Распаковать**. Указывает, что содержимое прикрепленных файлов необходимо распаковать для анализа.
- **Прикрепить**. Присоединяет образцы к объекту атрибуции.
- **Отменить**. Возврат к странице объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29) страница.

На этой странице доступны следующие действия: управление файлами, связанными с объектами атрибуции (см. раздел «Управление образцами, связанными с объектами атрибуции» на стр. 47).

kaspersky

Страница свойств объекта атрибуции

На странице свойств объекта атрибуции отображаются свойства объекта атрибуции.

Вы не можете изменять свойства объекта атрибуции для объектов атрибуции «Лаборатории Касперского».

Рисунок 13: Страница свойств объекта атрибуции

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).
2. Нажмите на имя объекта атрибуции.
3. Откроется страница свойств объекта атрибуции.

На этой странице есть три вкладки:

- **Информация**. Содержит общие свойства объекта атрибуции.
- **Образцы**. Содержит информацию о настраиваемых образцах, связанных с объектом атрибуции. Образцы, предоставленные «Лабораторией Касперского», не отображаются.
- **Вложение**. Содержит образец журнала вложений.

На этой странице доступны следующие действия:

- Управление объектами атрибуции (см. стр. 45).
- Управление файлами, связанными с объектами атрибуции (см. раздел «Управление образцами, связанными с объектами атрибуции» на стр. 47).

Вкладка **Информация**

Содержит общие свойства объекта атрибуции.

Элементы вкладки:

- **Имя**. Имя объекта атрибуции.
- **Родительский объект**. Имя родительского объекта атрибуции.
- **Предел генотипов**. Минимальное количество генотипов, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Если в выборке больше совпадающих генотипов, чем указанное число, эта сущность атрибуции отображается как аналогичная сущность атрибуции в выборке.
- **Предел строк**. Минимальное количество строк, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Если в выборке найдено больше совпадающих строк, чем указанное число, эта сущность атрибуции отображается как аналогичная сущность атрибуции в выборке.
- **Описание**. Описание объекта атрибуции.
- **Алиасы**. Список известных алиасов для этого объекта атрибуции.
- **Ссылки на отчеты**. Ссылки на отчеты, связанные с этим объектом атрибуции.
- **Комментарии**. Дополнительная информация о сущности атрибуции.

Вкладка **Образцы**

Содержит информацию об образцах, связанных с объектом атрибуции.

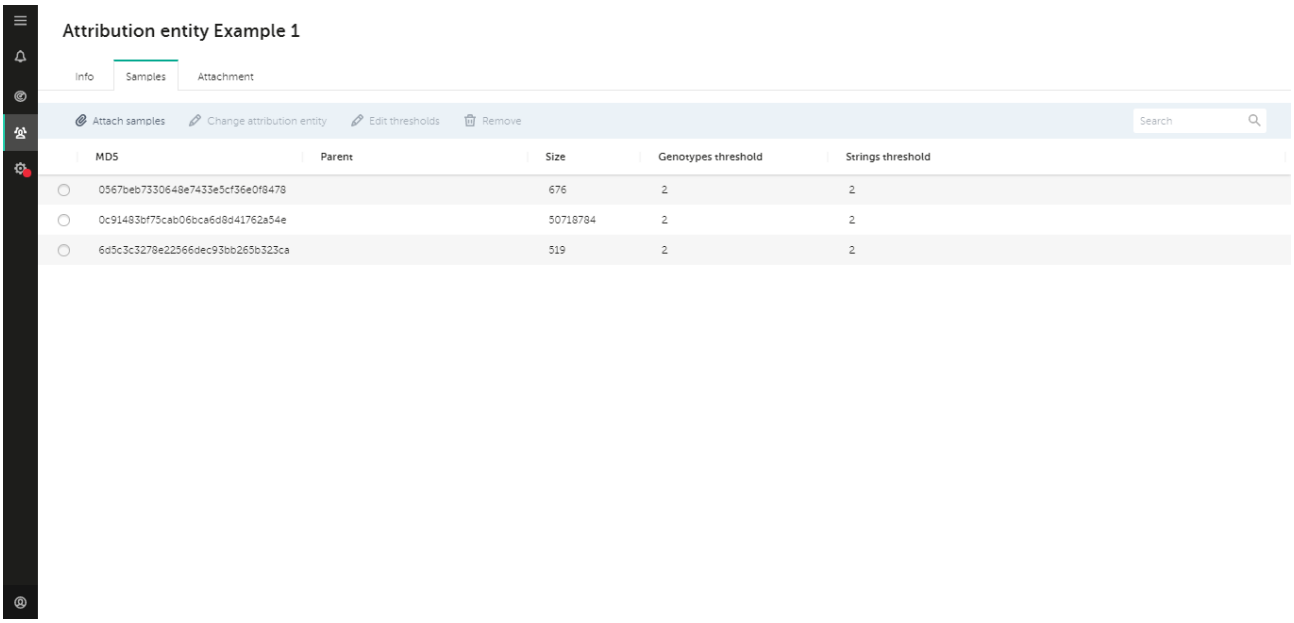

Рисунок 14: Вкладка Образцы

Элементы вкладки:

- **Прикрепить образцы**. Открывает страницу **Прикрепить образцы** (см. раздел «Прикрепить образцы» на стр. 33), где вы можете прикрепить образцы к этому объекту атрибуции.
- **Сменить объект атрибуции**. Присоединяет выбранный образец к другому объекту атрибуции.

- **Отредактировать пределы**. Редактирует минимальные уровни сходства для выбранного образца.
- **Удалить**. Удаляет выбранные образцы.
- **Искать**. Ищет список образцов по указанной строке.
- **Образцы**. Таблица, в которой отображаются все образцы для этого объекта атрибуции со связанной информацией.

В таблице образцов отображаются следующие данные:

- **Маркер выделения**. Нажмите на этот маркер, чтобы выбрать образец.
- **MD5**. MD5-хеш образца.
- **Родительский объект**. MD5-хеш родительского образца.
- **Размер**. Размер выборки в байтах.
- **Предел генотипов**. Минимальное количество генотипов, которые должны быть сопоставлены, чтобы отнести анализируемый образец к этому образцу.
- **Предел строк**. Минимальное количество строк, которые должны быть сопоставлены, чтобы отнести анализируемый образец к этому образцу.

Вкладка **Вложения**

Содержит образец журнала вложений.

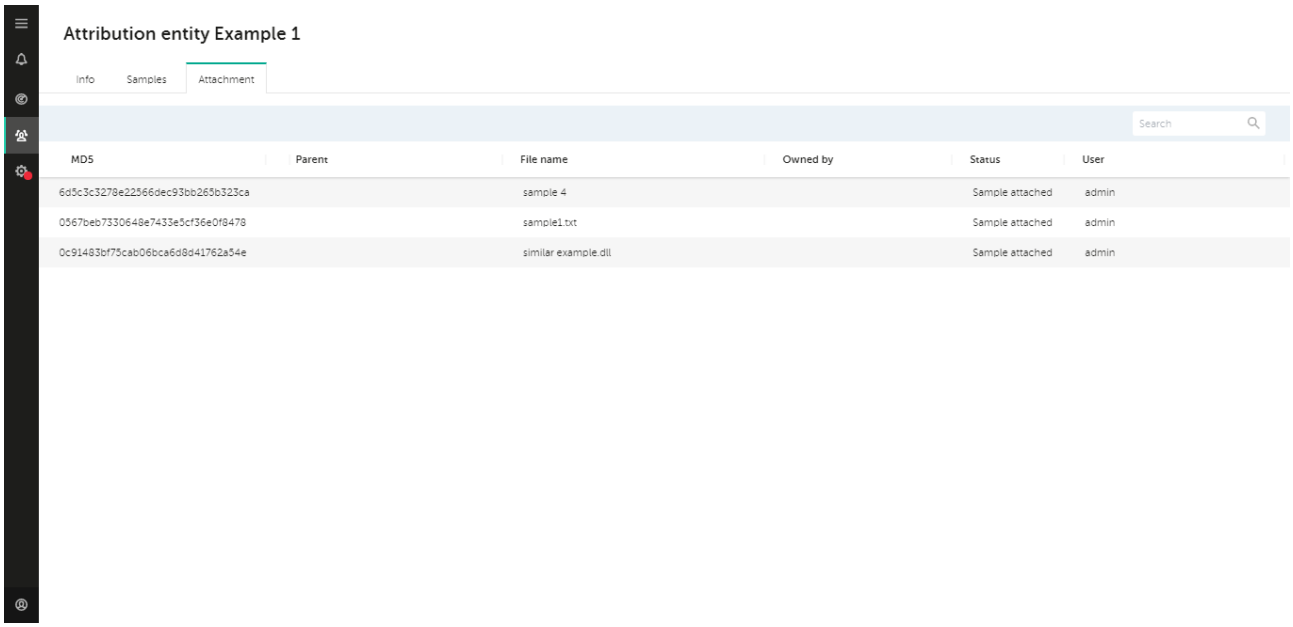

Рисунок 15: Вкладка "Вложения"

Элементы вкладки:

- **Журнал операций по прикреплению образцов**. Отображает все примеры операций с прикреплением для этого объекта атрибуции.
- **Отменить**. Если выполняется операция присоединения, вы можете отменить ее с помощью этого элемента.
- **Искать**. Ищет список операций с вложениями по MD5.

Журнал операций с вложениями отображает следующие данные:

- **MD5**. MD5-хеш образца.
- **Родительский объект**. MD5-хеш родительского образца.
- **Имя файла**. Имя файла сэмпла.
- **Статус**. Статус работы вложения.
- **Владелец**. Если образец принадлежит объекту атрибуции, отображается это имя объекта атрибуции.
- **Пользователь**. Пользователь, прикрепивший этот образец. Эта информация отображается только в том случае, если текущий пользователь является администратором.

Страница настроек

На странице настроек вы можете просмотреть информацию о лицензии и обновлениях, а также разрешить конфликты обновлений.

► *Чтобы перейти на эту страницу:*

1. В главном меню (см. стр. 21), выберите элемент **Настройки**.

   Откроется страница **Настройки**.

На этой странице доступны следующие действия: разрешение конфликтов обновлений (см. стр. 59).

Вкладка **Настройки**

На этой вкладке вы можете просмотреть информацию о версии KTAE, его базах и времени последнего обновления баз.

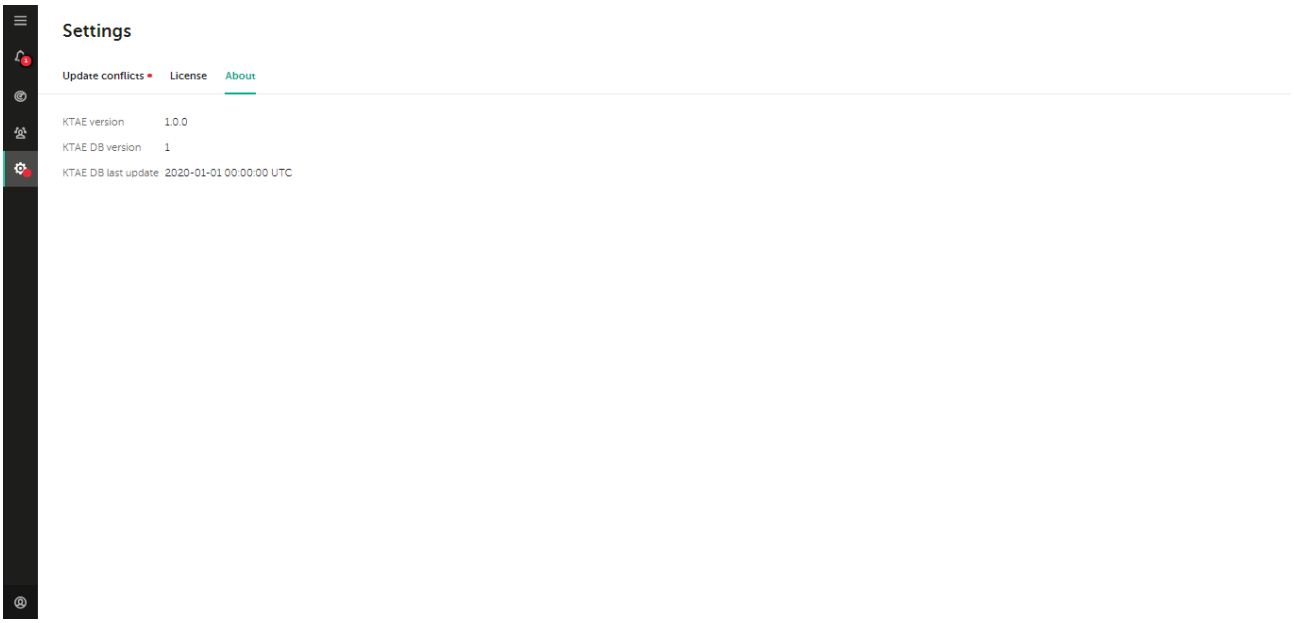

Рисунок 16: О вкладке

Эта вкладка содержит следующие элементы:

- **Версия KTAE**. Текущая версия Kaspersky Threat Attribution Engine.
- **Версия БД KTAЭ**. Текущая версия баз Kaspersky Threat Attribution Engine.
- **Последнее обновление БД KTAE (UTC)**. Время последнего обновления (UTC).

Вкладка **Лицензия**

На этой вкладке вы можете просмотреть информацию о лицензии KTAE.

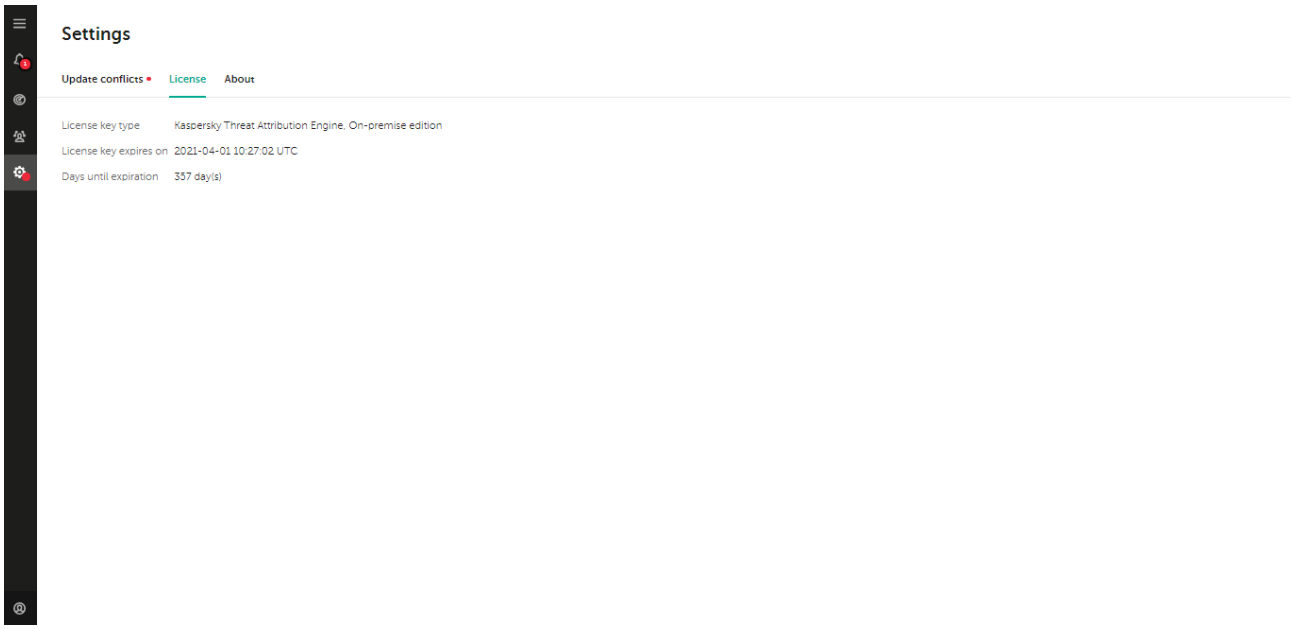

Рисунок 17: Вкладка "Лицензия"

Эта вкладка содержит следующие элементы:

- **Тип лицензионного ключа**. Тип лицензионного ключа.
- **Срок действия лицензионного ключа истекает**. Срок действия лицензионного ключа.
- **Дней до истечения срока**. Дней до истечения срока действия лицензионного ключа.
- **Максимум анализов в неделю**. Еженедельный лимит на количество анализов. Эта информация отображается, только если ваш тип лицензионного ключа имеет это ограничение.

Вкладка **Конфликты обновлений**

На этой вкладке вы можете просмотреть информацию о конфликтах обновлений.

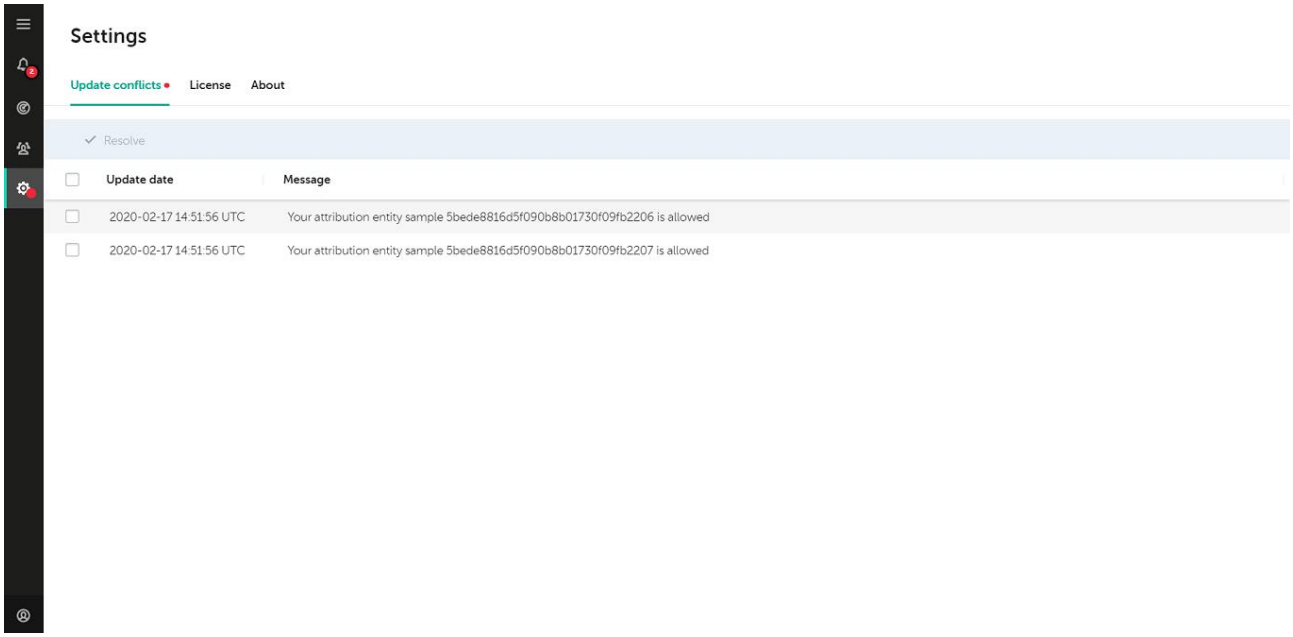

Рисунок 18: Вкладка "Конфликты обновлений"

На этой вкладке есть следующие элементы:

- **Разрешить конфликт**. Запускает разрешение конфликта обновлений для выбранных образцов.
- **Таблица конфликтов**. Отображает конфликты обновлений.

Таблица конфликтов

В таблице конфликтов обновлений отображается следующая информация о конфликтах обновлений:

- **Маркер выделения**. Нажатие на этот маркер выбирает конфликт обновления.
- **Дата обновления**. Время и дата обновления, вызвавшего конфликт. Время и дата в формате UTC.
- **Сообщение**. Описание конфликта обновления.

Вход в Kaspersky Threat Attribution Engine

В этом разделе описывается, как войти в Kaspersky Threat Attribution Engine через веб-интерфейс.

► *Чтобы войти в Kaspersky Threat Attribution Engine:*

1. В браузере перейдите по `адресу https: // localhost: 8080`.

   Откроется страница входа (см. раздел «Страница входа » на стр. 20)
2. Введите свой **логин** и **пароль**.

Для получения дополнительной информации о создании учетных записей пользователей см. раздел «Управление учетными записями пользователей» на стр. 55.

3. Нажмите на кнопку **Войти**.

Отправка файлов на анализ и атрибуцию

Kaspersky Threat Attribution Engine может анализировать файлы и находить объекты атрибуции, связанные с анализируемыми файлами. Когда вы отправляете файл на анализ, Kaspersky Threat Attribution Engine находит в этом файле генотипы и строки и сравнивает их с известными генотипами и строками. В результате этого сравнения Kaspersky Threat Attribution Engine может связать анализируемый файл с одним или несколькими известными объектами атрибуции.

О сущностях атрибуции

Сущность атрибуции - это субъект, кампания или известное вредоносное ПО. Эти три аспекта могут быть объединены в сущности атрибуции. Например, образец вредоносной программы может быть отнесен к известному субъекту APT, только если этот субъект использует именно это вредоносное ПО. В качестве другого примера, если анализируемый образец принадлежит популярной вредоносной программе, он будет отнесен к вредоносной программе, а не к конкретному субъекту.

О типах файлов, отправленных на анализ

Вы можете отправить на анализ следующие файлы:

- Любой тип файла размером от 6 байтов до 500 мегабайт (МБ).

  Поддерживаются файлы любого типа. Kaspersky Threat Attribution Engine может анализировать все типы исполняемых файлов и другие типы файлов, такие как файлы Portable Document Format (PDF), документы Microsoft Word, сценарии Java, файлы дампа памяти или файлы сертификатов.

- Архивы

  Kaspersky Threat Attribution Engine может распаковывать архивы, отправленные на анализ. Любой файл в архиве также должен иметь размер от 6 байт до 500 МБ при распаковке.

  Вы можете отправлять на анализ архивы, защищенные паролем. Поддерживаются следующие пароли: `инфицированный`, `вирус`, `вредоносный`, `чистый`, `111` и `123`.

  В одном архиве поддерживается максимум 1000 файлов. Если в архиве более 1000 файлов или истек тайм-аут для операции распаковки, в результатах анализа отображается предупреждение.

- Файлы дампа памяти

  Помимо типичных файлов, Kaspersky Threat Attribution Engine может также анализировать необработанные файлы дампа памяти и искать сходства с известными образцами объектов атрибуции. Например, вы можете создать файл дампа памяти в системе, которая, по вашему мнению, может быть скомпрометирована, и проанализировать ее в Kaspersky Threat Attribution Engine, чтобы выявить фрагменты вредоносного кода. Это может быть полезно во время реагирования на инциденты или когда система заражена бесфайловым вредоносным ПО.

  Поскольку файлы дампа памяти могут иметь размер нескольких гигабайт, для их анализа в Kaspersky Threat Attribution Engine вы должны выгружать дамп блоками размером до 500 МБ. Другой подход - извлечь запущенные процессы из файла дампа памяти в виде отдельных файлов с помощью внешнего инструмента, такого как Volatility, и проанализировать их отдельно. Это можно сделать с помощью Volatility и следующей команды:

```
volatility-2.2.standalone.exe -f% memdump.vmem% processingxedump --
dump-dir =% dumped_files_dir%
```

В приведенной выше команде замените `% memdump.vmem%` на имя файла дампа памяти, `% dumped_files_dir%` на путь к директории, в которой должны храниться полученные файлы.

Отправка файла на анализ и атрибуцию

► *Чтобы отправить файл на анализ и атрибуцию:*

1. Перейдите на страницу анализа (см. раздел «Страница анализа» на стр. 22).
2. Нажмите на кнопку **Новый анализ**.

   Откроется страница нового анализа (см. раздел «Страница нового анализа» на стр. 24).
3. Перетащите один или несколько файлов в зону **Перетащить файлы**. В качестве альтернативы нажмите на кнопку **Выбрать** и выберите файлы в окне браузера.

   У вашей учетной записи должны быть разрешения на чтение загруженного файла. В противном случае ваш браузер не сможет загрузить файл.
4. Если вы хотите игнорировать предельные значения сходства и включить все образцы с похожими генотипами и строками, установите флажок **Сбросить пределы сходства**.
5. Если вы хотите распаковать прикрепленный образец и проанализировать его содержимое, выберите элемент **Распаковать**.
6. Нажмите на кнопку **Пуск**.

   Откроется страница анализа (см. раздел «Страница анализа» на стр. 22).
7. Когда анализ будет завершен, просмотрите результаты, отображаемые на странице анализа (см. раздел «Страница анализа» на стр. 22).

Дополнительные сведения об интерпретации результатов анализа см. в разделе «Интерпретация результатов анализа» (см. стр. 42).

Интерпретация результатов анализа

В этом разделе приведены рекомендации по интерпретации результатов анализа.

Цели анализа

Цель анализа - определить следующую информацию:

- Субъект (группа или отдельное лицо), совершивший нападение
- Мотивация субъекта к нападению
- Тактика, приемы и процедуры субъекта (tactics, techniques, and procedures, TTP)

Если образец соответствует известному объекту атрибуции

Если Kaspersky Threat Attribution Engine обнаружит сходство между анализируемой выборкой и выборкой известного объекта атрибуции, вы должны ознакомиться с этим объектом атрибуции.

► *Чтобы узнать об известной сущности атрибуции:*

1. Просмотрите доступную информацию о сущности атрибуции в свойствах сущности атрибуции (см. раздел «Страница свойств сущности атрибуции» на стр. 35).
   - Описание объекта атрибуции содержит общую информацию о субъекте, кампании или вредоносном ПО.
   - Поле публичного отчета содержит ссылки на публичные отчеты, относящиеся к объекту атрибуции.
2. Дополнительную информацию об атрибуции можно получить на портале Kaspersky Threat Intelligence Portal. Портал Kaspersky Threat Intelligence предоставляет информацию о сопоставлении объекта атрибуции и связанных с ним правил Yara.

Количество объектов атрибуции в сопоставленных генотипах и строках

Для каждой совпадающей строки и генотипа вы можете проанализировать количество объектов атрибуции, которые используют этот генотип или строку:

- Сделайте приоритетным исследование строк и генотипов, используемых одним объектом атрибуции. Эти строки и генотипы специфичны для объекта атрибуции и могут помочь вам точно определить источник атаки.

Строки и генотипы с большим количеством объектов атрибуции, вероятно, принадлежат популярному вредоносному ПО, используемому многими участниками. Мы не рекомендуем приписывать такие строки и генотипы конкретному субъекту. Причина этого предостережения заключается в том, что такие строки и генотипы не могут быть надежно связаны с каким-либо конкретным субъектом.

Создание пользовательских объектов атрибуции

Используйте следующие рекомендации при создании пользовательских объектов атрибуции:

- Создайте настраиваемую сущность атрибуции для каждого инцидента.
- Если вы можете определить, что одна и та же группа совершает несколько атак, вы можете создать объект атрибуции для этой группы и назначить его родительским для всех связанных объектов атрибуции.
- Оставьте для пределов сходства значения по умолчанию. Изменяйте эти значения, только если есть проблемы с атрибуцией для объекта атрибуции.

Прикрепление образцов к объектам атрибуции

Используйте следующие рекомендации при прикреплении образцов к объектам атрибуции:

- Прикрепите образцы, которые необычны или уникальны для объекта атрибуции. Исполняемые файлы, сценарии и документы - самые эффективные образцы.
- Не прикрепляйте популярные файлы и файлы, относящиеся к законному программному обеспечению. Прикрепление файлов законного программного обеспечения может привести к ассоциации этого программного обеспечения с соответствующими объектами атрибуции. Чтобы проверить, является ли файл популярным или легитимным, используйте следующие сервисы: https://whitelisting.kaspersky.com. и https://opentip.kaspersky.com.

Разрешенные образцы, генотипы и строки

Образец, генотип или строка считаются *допустимыми,* если они связаны с файлом, помеченным «Лабораторией Касперского» как чистый или надежный. Разрешенные образцы, генотипы и строки

предоставляются с обновлениями баз Kaspersky Threat Attribution Engine. Пользователи Kaspersky Threat Attribution Engine не могут присвоить этот статус образцам, генотипам или строкам.

Возможные статусы анализа

Kaspersky Threat Attribution Engine может возвращать перечисленные ниже статусы анализа. Эти статусы отображаются в столбце **Top 5 похожих** на странице анализа (см. стр. 22).

Возможны следующие статусы:

- *Отменено*

  Анализ был отменен пользователем.

- *Допустимый образец*

  Анализируемый образец является разрешенным образцом.

- *Файл не найден*

  Произошла ошибка. Отправленный на анализ файл не найден на сервере.

- *Пустая экстракция*

  Никаких строк или генотипов из образца не извлечено.

- *Сходства не обнаружено*

  Ни одна из известных выборок объектов атрибуции не соответствует проанализированной выборке.

- *Не удалось извлечь*

  Произошла ошибка при извлечении строк и генотипов из выборки.

- *Размер недействителен*

  Размер анализируемой выборки не соответствует требованиям к размеру.

- *Дубликат*

  Образец имеет дубликаты в том же анализе.

- *Внутренняя ошибка*

  Произошла ошибка при анализе пробы.

Для распакованных образцов возможны следующие статусы:

- *Успешно*
- *Ошибка распаковки*
- *Не все распакованные образцы были обработаны, поскольку был достигнут предел количества распакованных файлов.*

kaspersky

Управление объектами атрибуции

В этом разделе описывается, как управлять объектами атрибуции, их свойствами и прикрепленными образцами.

О типах сущностей атрибуции

В Kaspersky Threat Attribution Engine есть два типа объектов атрибуции:

- Объекты атрибуции «Лаборатории Касперского» - данные объекта атрибуции предоставляются «Лабораторией Касперского».
- Пользовательские объекты атрибуции. Данные объекта атрибуции предоставляются вами.

В этом разделе

Управление объектами атрибуции «Лаборатории Касперского»

Атрибуты «Лаборатории Касперского» предоставляются «Лабораторией Касперского», поэтому они добавляются, обновляются и удаляются при обновлении баз Kaspersky Threat Attribution Engine.

► *Чтобы добавить комментарии к объектам атрибуции «Лаборатории Касперского»:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).
2. Выберите вкладку **Kaspersky**.
3. Выберите объект атрибуции, который вы хотите обновить, установив переключатель рядом с его именем.
4. Нажмите на кнопку **Редактировать**.
5. Откроется страница обновления объекта атрибуции (см. раздел «Страница обновления объекта атрибуции» на стр. 32).
6. Укажите комментарий в поле **Комментарии**.
7. Нажмите на кнопку **Изменить**.

kaspersky

Управление пользовательскими объектами атрибуции

Пользовательские объекты атрибуции - это объекты атрибуции, созданные вами, поэтому вы можете управлять ими следующими способами:

- Создать новые пользовательские объекты атрибуции
- Обновить существующие пользовательские объекты атрибуции
- Удалить существующие пользовательские объекты атрибуции

Указание информации для объекта атрибуции

Рекомендуем придерживаться следующих основных правил при указании информации о сущности атрибуции:

- Поле **Родительский объект** - используется для группировки нескольких объектов атрибуции под одним родительским объектом атрибуции. Например, если несколько атак имеют один источник, его можно указать как родительский объект атрибуции.
- Поле **Алиасы** - используется для хранения других известных имен объекта атрибуции. Например, если объект атрибуции является действующим лицом и имеет несколько известных алиасов, их можно указать в поле **Алиасы**.
- Поле **Ссылки отчета** - используется для ссылок на онлайн-публикации об этом объекте атрибуции.

Создание новой настраиваемой сущности атрибуции

► *Чтобы создать новую настраиваемую сущность атрибуции:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).
2. Выберите вкладку **Пользовательские**.
3. Нажмите на кнопку **Добавить**.
4. Откроется страница нового объекта атрибуции (см. раздел «Страница нового объекта атрибуции» на стр. 31).
5. Укажите все параметры для новой настраиваемой сущности атрибуции.
6. Нажмите на кнопку **Добавить**.
7. Если вы хотите прикрепить образцы к объекту атрибуции, см. раздел «Управление образцами, связанными с объектами атрибуции» на стр. 47.

Обновление настраиваемой сущности атрибуции

► *Чтобы обновить настраиваемый объект атрибуции:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).
2. Выберите вкладку **Пользовательские**.
3. Выберите объект атрибуции, который вы хотите обновить, установив переключатель рядом с его именем.
4. Нажмите на кнопку **Редактировать**.

Откроется страница обновления страницы объекта атрибуции (см. раздел «Обновление страницы объекта атрибуции» на стр. 32).

5. Измените свойства объекта атрибуции.
6. Нажмите на кнопку **Обновить**.
7. Чтобы обновить образцы, связанные с объектом атрибуции, см. раздел «Управление образцами, связанными с объектами атрибуции» на стр. 47).

Удаление настраиваемой сущности атрибуции

► *Чтобы удалить настраиваемый объект атрибуции:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).
2. Выберите вкладку **Пользовательские**.
3. Выберите объект атрибуции, который вы хотите удалить, установив переключатель рядом с его именем.
4. Нажмите на кнопку **Удалить**.

   Откроется окно **Удаление объекта атрибуции**.
5. Нажмите на кнопку **Удалить**.

Управление выборками, связанными с объектами атрибуции

Вы можете создавать и удалять образцы, связанные с настраиваемыми объектами атрибуции.

Прикрепление файлов к объекту атрибуции

► *Чтобы прикрепить файл к настраиваемому объекту атрибуции:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).
2. Нажмите на имя объекта атрибуции.

   Откроется страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).
3. Выберите вкладку **Образцы**.
4. Нажмите на кнопку **Прикрепить образцы**.
5. Откроется окно прикрепления образцов (см. раздел «Страница прикрепления образцов» на стр. 33).
6. Перетащите образец файла в зону **Перетащить файлы**. В качестве альтернативы нажмите на кнопку **Выбрать** и выберите файл в окне браузера.

   У вашей учетной записи должны быть разрешения на чтение загруженного файла. В противном случае ваш браузер не сможет загрузить файл.

7. Если вы хотите отключить распаковку прикрепленного образца, снимите флажок в поле **Распаковать**.
8. Нажмите на кнопку **Прикрепить**.
9. Образец будет загружен. Вы можете просмотреть статус вложения в объектах атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29) и на вкладке **Вложение** в свойствах объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр.35).

Удаление образцов

► *Чтобы удалить файл из настраиваемого объекта атрибуции:*

1. В главном меню (см. стр. 21) выберите элемент **Объекты атрибуции**.

   Откроется страница объектов атрибуции (см. раздел «Страница объектов атрибуции» на стр. 29).
2. На вкладке **Пользовательские** нажмите на имя объекта атрибуции.

   Откроется страница свойств объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35).
3. Откройте вкладку **Образцы**.
4. Выберите образец, который хотите удалить.
5. Нажмите на кнопку **Удалить**.
6. Подтвердите удаление образца.
7. Образец будет удален.

Возможные статусы прикрепленных образцов

Kaspersky Threat Attribution Engine может возвращать примеры статусов прикрепленных файлов, перечисленные ниже. Эти статусы отображаются на вкладке **Вложение** на странице свойств объекта атрибуции (см. стр. 35).

Возможны следующие статусы:

- *Отменено*

  Операция прикрепления была отменена пользователем.
- *Не удалось прикрепить образец*

  Произошла ошибка при прикреплении образца.
- *Допустимый образец*

  Образец не был прикреплен, потому что это разрешенный образец.
- *Файл не найден*

  Произошла ошибка. Отправленный для вложения файл не найден на сервере.
- *Пустая экстракция*

  Никаких строк или генотипов из образца не извлекали.
- *Не удалось извлечь*

  Произошла ошибка при извлечении строк и генотипов из выборки.
- *Образец прикреплен другим пользователем*

Этот образец прикреплен к объекту атрибуции другим пользователем.

- *Образец принадлежит другому объекту атрибуции*

  Образец уже принадлежит другому объекту атрибуции.

- *В образце разрешены только строки и генотипы*

  Разрешены все генотипы и строки, извлеченные из образца.

- *Размер недействителен*

  Размер анализируемой выборки не соответствует требованиям к размеру.

- *Сущность атрибуции не найдена*

  Сущность атрибуции удалена.

- *Внутренняя ошибка*

  Произошла ошибка при анализе пробы.

Для распакованных образцов возможны следующие статусы:

- *Успешно*
- *Ошибка распаковки*
- *Не все распакованные образцы были обработаны, поскольку был достигнут предел количества распакованных файлов.*

Скачивание отчетов

В этом разделе описывается информация, содержащаяся в отчетах, и рассказывается, как их загрузить.

Отчеты - это файлы, содержащие подробную информацию об анализах, созданные в формате TXT или JSON.

Для анализов, которые включают неупакованные образцы, все вложенные образцы, не имеющие сходства с известными образцами объектов атрибуции, исключаются из отчетов.

► *Чтобы скачать отчет в формате JSON:*

1. Перейдите на страницу анализа (см. раздел «Страница анализа» на стр. 22).
2. Нажмите на кнопку **JSON**.
3. Сохраните файл JSON в окне браузера.

► *Чтобы скачать отчет в формате TXT:*

1. Перейти на страницу анализа (см. раздел «Страница анализа» на стр. 22).
2. Нажмите на кнопку **TXT**.
3. Сохраните файл TXT в окне браузера.

Коды результатов

Отчеты содержат коды результатов, соответствующие результатам сканирования, отображаемым в интерфейсе. Дополнительные сведения о кодах результатов см. в разделе «Интерпретация результатов анализа» на стр. 42).

Таблица 4. Коды результатов

Код результата	Результат сканирования
100	Найдено сходство
101	Отменено
4	Допустимый образец
5	Файл не найден
6	Пустая экстракция
8	Сходства не обнаружено
10	Не удалось извлечь
15	Размер недействителен
16	Дубликат
500	Внутренняя ошибка

Статусы операций распаковки

Отчеты содержат коды операций распаковки, соответствующие статусам операций распаковки, отображаемым в интерфейсе.

Таблица 5. Коды результатов

Код результата	Результат сканирования
0	Успешно
1	Ошибка распаковки
2	Не все распакованные образцы были обработаны, поскольку был достигнут предел количества распакованных файлов.

Формат отчета JSON

Корневой уровень:

- Массив объектов анализа

Объекты анализа:

- **md5**: MD5-хеш анализируемого файла
- **filename**: Имя анализируемого файла
- **size**: Размер файла в байтах
- **top_5**: Массив с пятью первыми объектами атрибуции сущностей, у которых есть образцы, наиболее похожие на анализируемый образец:
  - **attribution_entity**: Имя объекта атрибуции

    - **similarity**: Процент сходства
- **matched_bad_genotypes**: Совпадение плохих генотипов. Количество генотипов в анализируемой выборке, совпадающих с генотипами в аналогичных выборках.
- **total_bad_genotypes**. Всего неверных генотипов. Количество генотипов в анализируемой выборке, которые соответствуют выборкам известных объектов атрибуции.
- **matched_bad_strings**: Совпадение неверных строк. Количество строк в анализируемой выборке, совпадающих со строками в аналогичных выборках.
- **total_bad_strings**. Всего неверных строк. Общее количество неверных строк в проанализированной выборке, которые совпадают с выборками известных объектов атрибуции.
- **result_code**: Код результата анализа, как описано выше в разделе «Коды результатов».
- **parent_md5**: MD5-хеш родительского файла анализируемого файла. Этот параметр используется для распакованных архивов.
- **extracted_path**: Путь внутри родительского файла к анализируемому файлу. Этот параметр используется для распакованных архивов.
- **unpacking_status**: Статус операции распаковки, как описано выше в разделе «Статусы распаковки».
- **Similar_samples**: Массив с похожими примерами объектов:
    - **md5**: MD5-хеш аналогичного образца.
    - **size**: Размер выборки в байтах.
    - **total_genotypes**: Общее количество генотипов в выборке.
    - **matched_genotypes_count**: Количество генотипов, соответствующих проанализированному образцу.
    - **total_strings**: Общее количество строк в сэмпле.
    - **matched_strings_count**: Количество генотипов, соответствующих проанализированному образцу.
    - **attribution_entity**: Имя объекта атрибуции, которому принадлежит образец.
    - **aliases**: Алиасы объекта атрибуции, которому принадлежит образец.
    - **similarity**: Процент сходства с анализируемым образцом.
- **matched_genotypes**: Массив объектов генотипов, соответствующих генотипам в выборке:
    - **genotype**: Генотип в образце, который соответствовал генотипам аналогичных образцов.
    - **matched**: Количество известных выборок объектов атрибуции, имеющих этот генотип.
    - **used_by**: Массив объектов атрибуции, которым принадлежат образцы с этим генотипом:
        - **attribution_entity**: Имя объекта атрибуции.
        - **matched**: Количество выборок данного объекта атрибуции, имеющих этот генотип.
- **matched_strings**: Массив строковых объектов, соответствующих генотипам в выборке:
    - **string**: Строка в образце, соответствующая генотипам аналогичных образцов.
    - **matched**: Количество известных образцов объектов атрибуции, имеющих эту строку.
    - **used_by**: Массив объектов атрибуции, которым принадлежат образцы с этой строкой:

- **attribution_entity**: Имя объекта атрибуции.
- **matched**: Эта строка содержит количество образцов этого атрибутивного объекта.

Формат отчета TXT

Отчет содержит строки со значениями, разделенными символом новой строки. Каждая строка представляет собой либо набор заголовков, разделенных точкой с запятой, либо набор значений для этих заголовков, разделенных точкой с запятой.

Информацию о данных, содержащихся в отчете, см. в описании соответствующих полей в разделе «Формат отчета JSON» выше.

Формат результата анализа:

- Заголовки верхнего уровня (одна строка)
- Значения для заголовков верхнего уровня (одна строка)
- Заголовки для похожих образцов (одна строка, с отступом)
- Значения для похожих образцов (одна или несколько строк с отступом)
- Заголовки для совпадающих генотипов (одна строка, с отступом)
- Значения для совпадающих генотипов (одна или несколько строк с отступом)
- Заголовки для совпадающих строк (одна строка, с отступом)
- Значения для совпадающих строк (одна или несколько строк с отступом)

kaspersky

Руководство администратора

В этом разделе представлена информация об использовании Kaspersky Threat Attribution Engine от имени администратора.

В этой главе

Об утилите admin_cli

В этом разделе описывается утилита admin_cli и ее использование.

Утилита admin_cli - это инструмент для управления административными задачами Kaspersky Threat Attribution Engine:

- Управление учетными записями пользователей (см. стр. 55)
- Обновление Kaspersky Threat Attribution Engine (см. раздел «Выполнение обновления» на стр. 57)
- Запуск и остановка службы Kaspersky Threat Attribution Engine (см. раздел «Управление службой Kaspersky Threat Attribution Engine» на стр. 56)
- Управление ключами API (см. раздел «Аутентификация REST API» на стр. 65)

Запуск утилиты admin_cli

► *Для запуска утилиты:*

1. Выполните следующую команду:

   ```
   bash / opt / ktae / bin / admin_cli
   ```

   Утилита подключается к базе данных, и команды в списке ниже становятся доступными.

2. Выполните необходимые команды из следующих:

   - `l , список`

     Отображает список пользователей и информацию о каждой учетной записи: идентификатор учетной записи пользователя, имя пользователя и роль пользователя.

- `c`, `создать`

  Создает нового пользователя.

  Использование: `создать`<login><username><password>

- `вверх`, `обновить-пароль`

  Обновляет пароль указанного пользователя.

  Использование: `update-password`<userId><password>

- `d`, `удалить`

  Удаляет учетную запись пользователя.

  Использование: `удалить`<userId>

- `ga`, `grant-admin`

  Назначает пользователю роль администратора.

  Использование: `grant-admin`<userId>

- `lk`, `listKeys`

  Выводит список всех ключей API.

- `ак`, `addKey`

  Добавляет ключ API для указанного пользователя.

  Использование: `addKey`<userId>

- `dk`, `deleteKey`

  Удаляет все ключи API для указанного пользователя.

  Использование: `deleteKey`<userId>

- `ck`, `checkKey`

  Проверяет действительность ключа API для указанного пользователя.

  Использование: `checkKey`<userId><api_key>

- `u`, `aggregate-update`

  Выполняет комбинированную операцию обновления. Обновляет базу данных и исполняемые файлы Kaspersky Threat Attribution Engine.

- `ud`, `updateData`

  Выполните обновление базы данных.

- `ub`, `updateBinaries`

  Выполните обновление двоичных файлов.

- `duu`, `deepunpack-update`

  Выполните обновление базы данных DeepUnpack.

- `ts`, `terminate-service`

  Останавливает службу Kaspersky Threat Attribution Engine.

- `rs`, `run-service`

Запускает службу Kaspersky Threat Attribution Engine.

- `q`, `quit`

  Выход из утилиты.

- `?`, `h`, `help`

  Отображает сообщение `справки`.

Управление учетными записями пользователей

В этом разделе описывается, как управлять учетными записями пользователей Kaspersky Threat Attribution Engine.

Вы можете создавать и удалять пользователей с помощью утилиты admin_cli.

О ролях пользователей

Kaspersky Threat Attribution Engine имеет следующие типы учетных записей пользователей:

- Учетная запись пользователя

  Имеет доступ к результатам анализа для аналитических операций, выполняемых с помощью этой учетной записи.

  Имеет доступ к образцам журналов вложений для образцов операций с вложениями, выполняемых с помощью этой учетной записи.

  Может удалять объекты атрибуции, созданные с помощью этой учетной записи.

- Учетная запись администратора

  Имеет доступ к результатам анализа для аналитических операций, выполняемых с помощью этой учетной записи.

  Имеет доступ к образцам журналов вложений для образцов операций с вложениями, выполненных с помощью любых учетных записей.

  Может удалять объекты атрибуции, созданные с помощью любых учетных записей.

  Имеет доступ к информации о конфликтах обновлений (см. раздел «Разрешение конфликтов обновлений » на стр.59).

Просмотр списка учетных записей пользователей

► *Чтобы просмотреть список учетных записей пользователей:*

1. Запустите утилиту admin_cli, как описано в разделе «Об утилите admin_cli» (см. стр. 53).
2. Выполните команду `списка`

   Утилита отображает список учетных записей пользователей с идентификатором учетной записи, именем пользователя и ролью пользователя для каждой учетной записи.

Создание учетной записи пользователя

► *Чтобы создать учетную запись пользователя:*

1. Запустите утилиту admin_cli, как описано в разделе «Об утилите admin_cli» (см. стр. 53).
2. Выполните команду `create`:

   ```
   Create <username> <login> <password>
   ```

   В приведенной выше команде:

   - Заменить `<username>` именем учетной записи пользователя. Это имя отображается в веб-интерфейсе.
   - Заменить `<login>` логином. Логин используется для входа в Kaspersky Threat Attribution Engine.
   - Заменить `<password>` паролем к учетной записи.
3. Если учетная запись должна иметь роль администратора, выполните команду `grant-admin`:

   ```
   grant-admin <userId>
   ```

   В приведенной выше команде замените `<userId>` идентификатором учетной записи пользователя.

Изменение пароля учетной записи пользователя

► *Чтобы изменить пароль учетной записи пользователя:*

1. Запустите утилиту admin_cli, как описано в разделе «Об утилите admin_cli» (см. стр. 53).
2. Выполните команду `update-password`:

   ```
   update-password <userId><password>
   ```

   В приведенной выше команде замените<userId> на идентификатор учетной записи пользователя и замените `<password>` новым паролем.

Управление сервисом Kaspersky Threat Attribution Engine

Вы можете запускать и останавливать службу Kaspersky Threat Attribution Engine с помощью утилиты admin_cli.

Запуск сервиса Kaspersky Threat Attribution Engine

► *Чтобы запустить службу Kaspersky Threat Attribution Engine:*

1. Запустите утилиту admin_cli, как описано в разделе «Об утилите admin_cli» (см. стр. 53).
2. Выполните команду `start-service`:

```
start-service
```

Остановка службы Kaspersky Threat Attribution Engine

► *Чтобы остановить службу Kaspersky Threat Attribution Engine:*

1. Запустите утилиту admin_cli, как описано в разделе «Об утилите admin_cli» (см. стр. 53).
2. Выполните команду `stop-service`:

   ```
   stop-service
   ```

Выполнение обновления

Сценарий обновления включает обновление бинарных файлов и баз Kaspersky Threat Attribution Engine.

Мы рекомендуем обновлять Kaspersky Threat Attribution Engine каждые 14 дней.

Проверить время последнего обновления баз можно на странице настроек (см. раздел «Страница настроек» на стр. 38).

Обновление Kaspersky Threat Attribution Engine происходит пошагово:

1. Выполните резервное копирование базы данных, как описано в разделе «Шаг 1. Резервное копирование базы данных» на стр. 57.
2. Загрузите обновления, как описано в разделе «Шаг 2. Скачивание обновлений» на стр. 58.
3. Обновите Kaspersky Threat Attribution Engine, как описано в разделе «Шаг 3. Запуск обновления» на стр. 59.

Если на любом шаге возникнут конфликты обновлений, вы сможете их разрешить (см. раздел «Разрешение конфликтов обновлений» на стр. 59 и раздел «Страница настроек» на стр. 38).

В этом разделе

Шаг 1. Резервное копирование базы данных

Перед обновлением Kaspersky Threat Attribution Engine вам может потребоваться создать резервную копию базы данных. Процедура резервного копирования может помочь вам избежать потенциальной потери личных данных.

Методы резервного копирования базы данных

Мы рекомендуем следующие методы резервного копирования базы данных:

- Для таблиц размером более 100 мегабайт (МБ) используйте команду `FLUSH TABLES` table_name... `FOR EXPORT`.

  Дополнительные сведения об этой команде см. в справочном руководстве MySQL 8.0.
- Для таблиц размером менее 100 МБ используйте клиентскую утилиту mysqldump.

  Дополнительные сведения об этой утилите см. в справочном руководстве MySQL 8.0..

Таблицы базы данных для резервного копирования

Мы рекомендуем сделать резервную копию следующих таблиц:

- customer_attribution_entity_sample_genotypes
- customer_attribution_entity_sample_strings
- customer_attribution_entity_samples
- attribution_entities
- analyzing_samples
- analyzing_sample_genotypes
- analyzing_sample_strings
- analyzing_sample_similar_samples
- analyzing_sample_statistic
- locked_files
- attaching_samples
- users
- sessions
- credentials
- api_keys
- conflicts
- update_metadata
- flyway_schema_history

Шаг 2. Скачивание обновлений

Вы можете скачать обновления для Kaspersky Threat Attribution Engine с помощью скрипта. После загрузки обновлений их необходимо перенести в защищенный периметр.

► *Чтобы скачать обновления для Kaspersky Threat Attribution Engine:*

1. В открытом периметре перейдите в следующую директорию:

   ```
   cd / opt / ktae-updater /
   ```

2. В открытом периметре запустите скрипт, скачивающий обновления:

   ```
   ./download_all.sh OUTPUT_DIR
   ```

   В приведенном выше примере команды замените `OUTPUT_DIR` на директорию, в которой вы хотите хранить загруженные файлы.

3. Перенесите загруженные файлы в безопасный периметр вручную.

   Сохраните структуру директорий, как она представлена в `OUTPUT_DIR`.

4. Скопируйте переданные файлы в директорию, в которой находится утилита admin_cli, используемая для обновления (см. раздел «Об утилите admin_cli» на стр. 53).

   Эта директория указана в блоке обновлений в конфигурационном файле утилиты admin_cli.

Возможные ошибки

Если лицензионный ключ DeepUnpack недействителен, возникает следующая ошибка:

```
Не удается инициализировать движок. Проблема с лицензией. Не удалось загрузить обновления DeepUnpack! Код результата: 93.
```

Шаг 3. Запуск обновления

Обновление Kaspersky Threat Attribution Engine включает в себя обновление двоичных файлов Kaspersky Threat Attribution Engine, обновление баз Kaspersky Threat Attribution Engine и обновление баз DeepUnpack. Вы можете выполнить эти операции с помощью утилиты admin_cli.

► *Чтобы обновить Kaspersky Threat Attribution Engine:*

1. Запустите утилиту admin_cli, как описано в разделе «Об утилите admin_cli» (см. стр. 53).
2. В утилите admin_cli выполните команду `terminate-service`.
3. В утилите admin_cli выполните команду `aggregate-update`.

   Чтобы обновить только двоичные файлы Kaspersky Threat Attribution Engine, выполните команду `updateData`.

   Чтобы обновить только базы Kaspersky Threat Attribution Engine, выполните команду `updateBinaries`.

   Чтобы обновить только базы данных DeepUnpack, выполните команду `deepunpack-update`.

4. В утилите admin_cli выполните команду `run-service`.

Разрешение конфликтов обновлений

В этом разделе объясняется, что такое конфликты обновлений и как их разрешать.

О конфликтах обновлений

Конфликт обновления возникает, когда разрешенные образцы, предоставленные новым обновлением, совпадают с существующими образцами, прикрепленными к объекту атрибуции. В этом случае Kaspersky Threat Attribution Engine не сможет разрешить этот конфликт самостоятельно. Вы должны решить, считается ли образец разрешенным или нет.

Конфликты обновлений не блокируют операцию обновления. Если возникли конфликты обновлений, Kaspersky Threat Attribution Engine все равно обновит свои базы.

Об уведомлениях о конфликтах обновлений

Если у Kaspersky Threat Attribution Engine есть активные конфликты обновлений, он отображает уведомление ( ) для учетных записей администратора в главном меню (см. стр. 21).

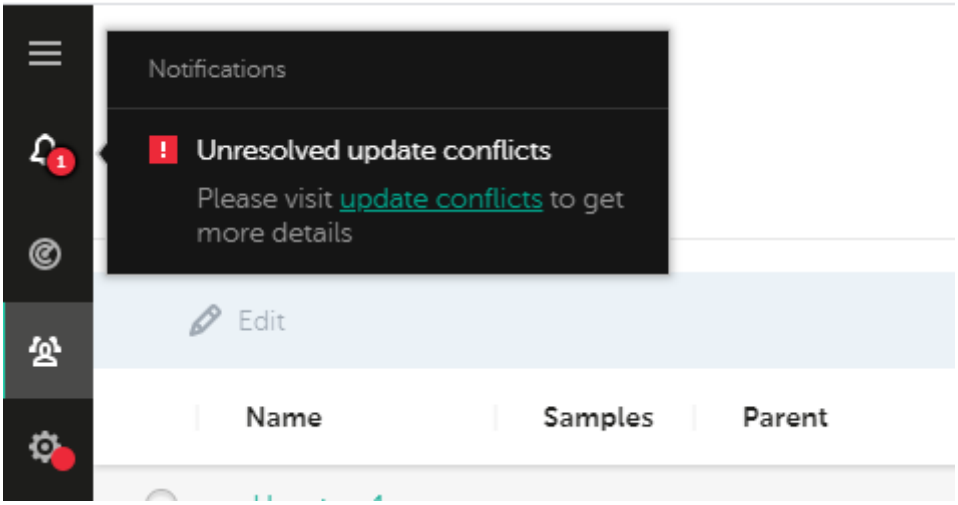

Рисунок 19: Уведомление о конфликтах обновлений

Разрешение конфликтов обновлений

Администратор может разрешить конфликты обновлений на странице настроек.

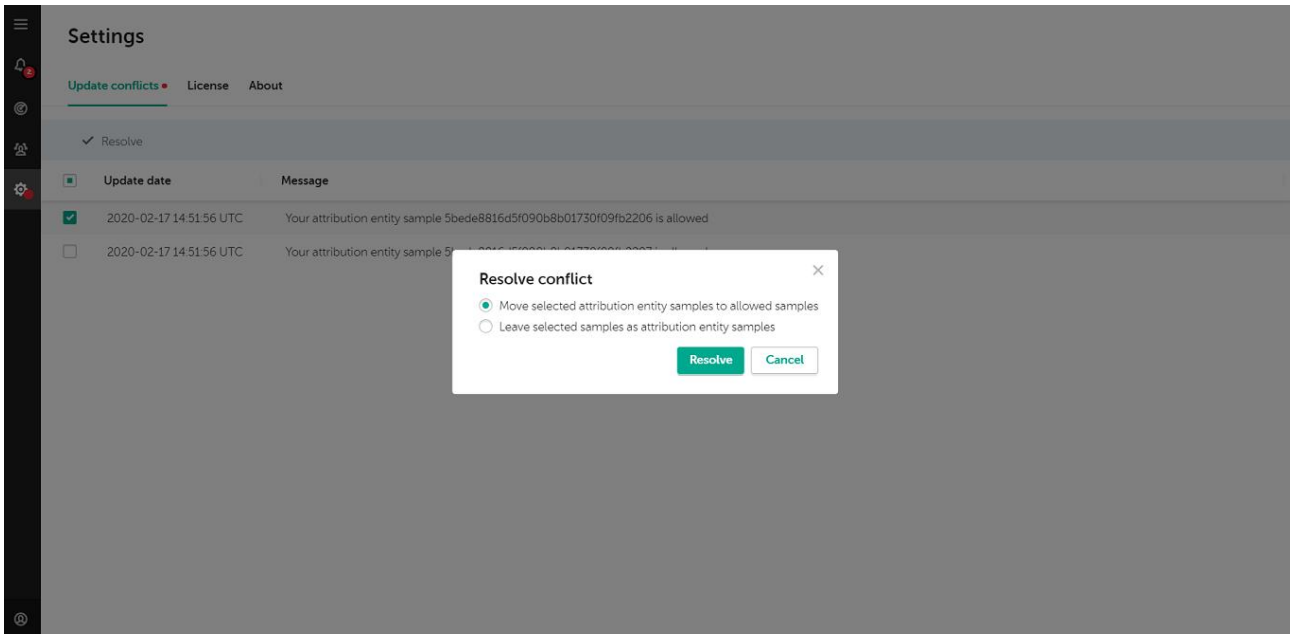

Рисунок 20: Окно разрешения конфликта

► *Чтобы разрешить конфликт обновления:*

1. Войдите в Kaspersky Threat Attribution Engine как администратор.
2. Перейдите на страницу настроек (см. раздел «Страница настроек» на стр. 38).
3. Выберите вкладку **Конфликты обновлений**.

   На вкладке отображается список конфликтов обновлений и даты обновлений.
4. Установите флажки для конфликтов обновлений, которые вы хотите разрешить.

   Вы также можете нажать на контрольную сумму MD5, чтобы перейти к свойствам объекта атрибуции (см. раздел «Страница свойств объекта атрибуции» на стр. 35), вызвавшего конфликт.
5. Нажмите на кнопку **Разрешить**.

   Откроется окно **Разрешение конфликтов**.
6. Выберите вариант разрешения выбранных конфликтов:
   - Переместить выбранные образцы сущностей атрибуции в разрешенные образцы.

     Выберите этот параметр, чтобы отделить выбранные образцы от их текущих объектов атрибуции и переместить их в разрешенные образцы.
   - Оставить выбранные образцы как образцы объектов атрибуции.

     Выберите этот параметр, чтобы сохранить выбранные образцы прикрепленными к их текущим объектам атрибуции. Kaspersky Threat Attribution Engine не считает образцы разрешенными.
7. Нажмите на кнопку **Разрешить**.

О лицензировании

В этом разделе объясняется, как работает лицензирование в Kaspersky Threat Attribution Engine.

О токенах

Лицензионная информация (лицензионный ключ) Kaspersky Threat Attribution Engine хранится на токене. Этот токен должен присутствовать для работы Kaspersky Threat Attribution Engine.

Об ограничениях лицензионного ключа

У каждого лицензионного ключа есть срок действия. Если срок действия лицензионного ключа истекает, вы больше не сможете выполнять анализ и прикреплять образцы к объектам атрибуции.

Некоторые типы лицензионных ключей имеют ограничение на максимальное количество анализируемых файлов в неделю. Когда вы отправляете файлы на анализ, они распаковываются (при необходимости) и подсчитывается общее количество уникальных файлов. Это число вычитается из еженедельной квоты для анализируемых файлов. Квота уменьшается на каждый анализ. Например, если вы повторно отправите тот же архив на анализ, еженедельная квота для анализируемых файлов будет снова уменьшена на количество уникальных файлов в архиве.

О статусах лицензионных ключей

Kaspersky Threat Attribution Engine периодически проверяет лицензионную информацию, хранящуюся в токене.

В зависимости от статуса лицензионной информации Kaspersky Threat Attribution Engine выполняет следующие действия:

- Лицензионного ключа нет.

  Вы больше не можете выполнять анализ и прикреплять образцы к объектам атрибуции.

  Kaspersky Threat Attribution Engine не обновляется.

- Срок действия лицензионного ключа истек.

  Вы больше не можете выполнять анализ и прикреплять образцы к объектам атрибуции.

  Kaspersky Threat Attribution Engine не обновляется. Обратитесь в Службу технической поддержки (см. раздел «Как получить техническую поддержку» на стр. 89), чтобы получить новый лицензионный ключ.

- Лицензионный ключ временно заблокирован.

  Чтобы удалить этот статус, выполните действия, описанные в разделе «Удаление временно заблокированного статуса» ниже.

- Лицензионный ключ заблокирован.

  Лицензионный ключ, хранящийся в токене, больше не может быть использован. Вы должны получить новый токен. Обратитесь в службу технической поддержки (см. раздел «Как получить техническую поддержку» на стр.89).

Удаление временно заблокированного статуса

► *Чтобы снять статус временно заблокированного с лицензионного ключа:*

1. На компьютере, где установлен Kaspersky Threat Attribution Engine, укажите правильную дату и время.
2. Перезапустите Kaspersky Threat Attribution Engine. (см. раздел «Управление сервисом Kaspersky Threat Attribution Engine» на стр. 56).

О правах доступа к директории

В этом разделе объясняется, как Kaspersky Theat Attribution Engine назначает права доступа к директориям.

По умолчанию Kaspersky Theat Attribution Engine ограничивает доступ ко всем своим файлам одной учетной записи пользователя в системе, которая используется Kaspersky Theat Attribution Engine. Только эта учетная запись пользователя и учетная запись root имеют права на чтение, запись и удаление файлов Kaspersky Theat Attribution Engine.

После установки продукта мы рекомендуем вам отслеживать и контролировать права, назначенные другим учетным записям пользователей в системе. Это может предотвратить возможные проблемы при работе с Kaspersky Theat Attribution Engine.

kaspersky

Работа с сертификатами

В этом разделе объясняется, как сертификаты работают в Kaspersky Theat Attribution Engine.

О сертификате по умолчанию

По умолчанию Kaspersky Theat Attribution Engine использует самозаверенный сертификат для Transport Layer Security (TLS).

Когда пользователь впервые открывает веб-интерфейс Kaspersky Theat Attribution Engine в браузере, ему предоставляется информация о самозаверенном сертификате и предлагается его добавить. Рекомендуется добавить сертификат в список доверенных сертификатов.

Если такая же подсказка появится позже, пользователь должен прекратить работу с Kaspersky Theat Attribution Engine и обратиться к администратору. Это может указывать на потенциальную проблему безопасности.

Использование собственных сертификатов

Вы можете настроить Kaspersky Theat Attribution Engine на использование настраиваемого сертификата. Например, этот сертификат может быть подписанным сертификатом, используемым в вашей организации.

► *Чтобы настроить Kaspersky Theat Attribution Engine на использование настраиваемого сертификата:*

1. Поместите сертификат в формате PKCS12 в директорию, в которой Kaspersky Theat Attribution Engine будет его использовать.

   По умолчанию Kaspersky Theat Attribution Engine использует сертификат, расположенный в директории / opt / ktae / cert.
2. Откройте конфигурационный файл Kaspersky Theat Attribution Engine с именем /opt/ktae/conf/application.conf.
3. В разделе `tls-settings`:
   - Укажите путь к сертификату в параметре `key-store-path`.
   - Укажите пароль для сертификата в параметре `key-store-password`.

Удаление KTAE

В этом разделе объясняется, как удалить Kaspersky Threat Attribution Engine.

► *Чтобы удалить Kaspersky Threat Attribution Engine:*

1. Выполните следующие действия в охраняемом периметре:
   a. Остановите службы ktae и kavehost, выполнив следующие команды:

      ```
      systemctl stop ktae kavehost
      /etc/init.d/kavehost stop
      ```

b. Удалите RPM-пакет Kaspersky Threat Attribution Engine, выполнив следующую команду:

```
rpm -e ktae-bin
```

c. Подключитесь к базе данных Kaspersky Threat Attribution Engine.

Параметры для подключения к базе данных вы можете найти в конфигурационном файле утилиты admin_cli (см. раздел «Об утилите admin_cli» на стр. 53).

d. Удалите базу данных Kaspersky Threat Attribution Engine, выполнив следующую команду:

```
drop database ktae_ext;
```

e. Удалите директорию, в которой был установлен Kaspersky Threat Attribution Engine, чтобы удалить оставшиеся файлы.

По умолчанию, это директория `/ opt / ktae`.

2. В открытом периметре удалите директорию, в которой был установлен Kaspersky Threat Attribution Engine.

По умолчанию, это директория `/ opt / ktae-updater`.

kaspersky

Справочник по REST API

В этом разделе представлена информация о REST API Kaspersky Threat Attribution Engine.

В этой главе

Аутентификация REST API

KTAE REST API-аутентификация основана на API-ключах. Это означает, что вы должны получить ключ API для своей учетной записи. Затем вы сможете делать запросы, используя этот ключ для аутентификации.

Создание ключа API

Используйте утилиту admin_cli, чтобы создать ключ API для учетной записи пользователя.

Мы рекомендуем вам создать отдельную учетную запись пользователя, которая будет взаимодействовать только с Kaspersky Threat Attribution Engine API. Не выполняйте вызовы API с помощью учетной записи, которую вы используете для регулярного взаимодействия с Kaspersky Threat Attribution Engine.

► *Чтобы создать ключ API:*

1. Запустите утилиту admin_cli, как описано в разделе «Об утилите admin_cli» (см. стр. 53).
2. Выполните команду `addKey`:

   ```
   addKey <userId>
   ```

   В приведенной выше команде замените `<userId>` идентификатором учетной записи пользователя.

Аутентификация с использованием ключа API

► *Для аутентификации с использованием ключа API:*

1. Добавьте заголовок `Api-Key` в заголовок запроса. Используйте следующий формат:

   ```
   API-key: <key>
   ```

2. Сделайте любой запрос API и проверьте статус ответа:
   - Статус `200` означает, что запрос был успешным.

- Статус `401` означает, что ваша попытка авторизации не удалась.

Проверка действительности ключа API

► *Чтобы проверить действительность ключа API:*

1. Запустите утилиту admin_cli, как описано в разделе «Об утилите admin_cli» (см. стр. 53).
2. Выполните команду `checkKey`:

   ```
   checkKey <userId> <api_key>
   ```

   В приведенной выше команде замените `<userId>` идентификатором учетной записи пользователя.

   В приведенной выше команде замените `<api_key>` значением ключа API.

Удаление ключей API для учетной записи пользователя

► *Чтобы удалить все ключи API для учетной записи пользователя:*

1. Запустите утилиту admin_cli, как описано в разделе «Об утилите admin_cli». (см. стр. 53).
2. Выполните команду `deleteKey`:

   ```
   deleteKey <userId>
   ```

   В приведенной выше команде замените `<userId>` идентификатором учетной записи пользователя.

Методы

В этом разделе описаны методы, доступные в REST API Kaspersky Threat Attribution Engine.

В этом разделе

kaspersky

Образцы POST

Присоединяет образцы к указанной сущности атрибуции.

Путь

`/api/samples/{entityName}`

Операция

`POST`

Параметры запроса

Этот запрос имеет следующие параметры:

Таблица 6. Параметры запроса образцов

Имя	Обязательный	Тип параметра	Тип значения		Описание
`entityName`	Да	Путь	`string`		Имя объекта атрибуции. Образец будет прикреплен к этому объекту атрибуции.
`unpack`	Нет	Запрос	`boolean`		Флаг, разрешающий распаковку. Значение по умолчанию: `false`.

Тело запроса

Этот запрос имеет следующее тело запроса:

Тип носителя: `multipart / form-data`.

Таблица 7. Тело запроса образцов

Имя	Тип значения	Формат значения	Описание
`data`	`string`	`binary`	Содержимое файла.

Ответы

На этот запрос есть следующие ответы.

Таблица 8. Образцы ответов на запросы

Код	Тип носителя	Схема ответа	Описание
200	application/json	ApiResponse (см. стр. 72)	ОК Образец был успешно прикреплен.
401	application/json	ErrorResponse (см. стр. 72)	Несанкционированный запрос. Авторизуйтесь с помощью ключа API (см. раздел «Аутентификация REST API » на стр. 65).
500	application/json	ErrorResponse (см. стр. 72)	Ошибка сервера. Ответ содержит описание ошибки.

Атрибуция POST

Создает новую сущность атрибуции.

Путь

`/api/attribution-entity`

Операция

`POST`

Параметры запроса

Этот запрос не имеет параметров.

Тело запроса

Этот запрос имеет следующее тело запроса.

Тип носителя: `application/json`.

Таблица 9. Тело запроса объекта атрибуции

Имя	Обязательный	Схема	Описание
AttributionEntity	Да	AttributionEntity (см. стр. 73)	Параметры объекта атрибуции.

Ответы

На этот запрос есть следующие ответы.

Таблица 10. Ответы на запросы атрибуции

Код	Тип носителя	Схема ответа	Описание
200	application/json	ApiResponse (см. стр. 72)	ОК Сущность атрибуции была успешно создана.
400	application/json	ErrorResponse (см. стр. 73)	Неверный запрос. Указанные параметры объекта атрибуции недействительны.
401	application/json	ErrorResponse (см. стр. 72)	Несанкционированный запрос. Авторизуйтесь с помощью ключа API (см. раздел «Аутентификация REST API » на стр. 65).
500	application/json	ErrorResponse (см. стр. 72)	Ошибка сервера. Ответ содержит описание ошибки.

Отчет GET

Получает данные отчета в указанном формате.

Путь

`/api/report`

Операция

`GET`

Параметры запроса

Этот запрос имеет следующие параметры.

Таблица 11. Параметры запроса отчета

Имя	Обязательный	Тип параметра	Тип значения	Описание
format	Да	Запрос	string	Формат отчета. Возможные значения: json. Значение по умолчанию: json.

Ответы

На этот запрос есть следующие ответы.

Таблица 12. Ответы на запросы отчета

Код	Тип носителя	Схема ответа	Описание
200	application/json	ReportData (см. стр. 82)	ОК Отчет был успешно создан.
401	application/json	ErrorResponse (см. стр. 72)	Несанкционированный запрос. Авторизуйтесь с помощью ключа API (см. раздел «Аутентификация REST API » на стр. 65).
500	application/json	ErrorResponse (см. стр. 72)	Ошибка сервера. Ответ содержит описание ошибки.

Анализ POST

Начинает новый анализ.

Путь

`/api/analysis`

Операция

`POST`

Параметры запроса

Этот запрос имеет следующие параметры.

Таблица 13. Параметры запроса на анализ

Имя	Обязательный	Тип параметра	Тип значения	Описание
resetThreshold	Нет	Запрос	boolean	Флаг игнорирования предельных значений схожести для сравниваемых образцов. Значение по умолчанию: `false`.
unpack	Нет	Запрос	boolean	Флаг, разрешающий распаковку. Значение по умолчанию: `true`.

Тело запроса

Этот запрос имеет следующее тело запроса.

Тип носителя: `multipart / form-data`.

Таблица 14. Тело запроса на анализ

Имя	Тип значения	Формат значения	Описание
`data`	`string`	`binary`	Содержимое файла.

Ответы

На этот запрос есть следующие ответы.

Таблица 15. Ответы на запросы анализа

Код	Тип носителя	Схема ответа	Описание
`200`	`application/json`	`ApiResponse` (см. стр. 72)	ОК Анализ был успешно создан.
`401`	`application/json`	`ErrorResponse` (см. стр. 72)	Несанкционированный запрос. Авторизуйтесь с помощью ключа API (см. раздел «Аутентификация REST API » на стр.65).
`500`	`application/json`	`ErrorResponse` (см. стр. 72)	Ошибка сервера. Ответ содержит описание ошибки.

Модели данных (схемы)

В этом разделе описаны модели (схемы) данных, доступные в REST API Kaspersky Threat Attribution Engine.

В этом разделе

kaspersky

ApiResponse

Содержит ответные сообщения API.

Синтаксис

```
ApiResponse {
    message string
}
```

Пример

```
{
    "message": "string"
}
```

Свойства

Эта модель данных имеет следующие свойства.

Таблица 16. Свойства ApiResponse

Имя	Обязательный	Множественный	Тип значения	Описание
message	Нет	Нет	string	Ответное сообщение API.

ErrorResponse

Содержит описание ошибки.

Синтаксис

```
ApiResponse {
    error string
}
```

Пример

```
{
  "error": "Error description"
}
```

Свойства

Эта модель данных имеет следующие свойства.

Таблица 17. Свойства ErrorResponse

Имя	Обязательный	Множественный	Тип значения	Описание
`error`	Нет	Нет	`string`	Описание ошибки.

ErrorsResponse

Содержит описание нескольких ошибок.

Пример

```
{
    "error": [
        "Error description",
        "Another error description"
    ]
}
```

Свойства

Эта модель данных имеет следующие свойства.

Таблица 18. Свойства ErrorsResponse

Имя	Обязательный	Множественный	Тип значения	Описание
`error`	Нет	Да	`string`	Описание ошибки.

AttributionEntity

Содержит свойства объекта атрибуции.

Пример

```
{
  "name": "entity",
  "parent": "parent",
  "description": "Entity description",
  "comments": "Comment text",
  "minSimGenotypesThreshold": 2,
  "minSimStringsThreshold": 2,
  "reportLinks":
"https://reports.example.com/entity,https://reports.example.com/aliasentit
y",
  "aliases": "aliasentity"
}
```

Свойства

Эта модель данных имеет следующие свойства.

Таблица 19. Свойства AttributionEntity

Имя	Обязательный	Множественный	Тип значения	Описание
`name`	Да	Нет	`string`	Имя объекта атрибуции.
`parent`	Нет	Нет	`string`	Название родительского объекта атрибуции.
`description`	Нет	Нет	`string`	Описание объекта атрибуции.
`comments`	Нет	Нет	`string`	Комментарий объекта атрибуции.
`minSimGenesThreshold`	Нет	Нет	`integer`	Предел генотипов. Минимальное количество генотипов, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Значение по умолчанию - `2`.

Имя	Обязательный	Множественный	Тип значения	Описание
`minSimStringsThreshold`	Нет	Нет	`integer`	Предел строк. Минимальное количество строк, которые должны быть сопоставлены, чтобы отнести образец к этому объекту атрибуции. Если в выборке найдено больше совпадающих строк, чем указанное число, эта сущность атрибуции отображается как аналогичная сущность атрибуции в выборке. Значение по умолчанию - `2`.
`reportLinks`	Нет	Нет	`string`	Ссылки на отчеты об этой атрибуции. Ссылки на несколько отчетов разделяются запятой (`,`).
`aliases`	Нет	Нет	`string`	Известные алиасы для этого объекта атрибуции.

UsedByData

Содержит информацию об объектах атрибуции, использующих генотип или строку из анализируемой выборки.

Пример

```
{
    "attribution_entity": "entity1",
    "matched": 2
}
```

Свойства

Эта модель данных имеет следующие свойства.

Таблица 20. Свойства UsedByData

Имя	Обязательный	Множественный	Тип значения	Описание
`attribution_entity`	Да	Нет	`string`	Имя объекта атрибуции.
`matched`	Да	Нет	`integer`	Количество образцов объектов атрибуции, которые имеют этот генотип или строку.

Top5Data

Содержит информацию о сущности атрибуции, аналогичной анализируемой сущности атрибуции.

пример

```
{
    "attribution_entity": "entity1",
    "similarity": 100
}
```

Свойства

Эта модель данных имеет следующие свойства.

Таблица 21. Top5Data свойства

Имя	Обязательный	Множественный	Тип значения	Описание
`attribution_entity`	Да	Нет	`string`	Имя объекта атрибуции.
`matched`	Да	Нет	`integer`	Процент сходства.

SimilarData

Содержит информацию об образце, аналогичном проанализированному образцу.

Пример

```
{
      "md5": "44d88612fea8a8f36de82e1278abb02f",
      "size": 128,
      "matched_genotypes_count": 1
      "total_genotypes": 1,
      "matched_strings_count": 1,
      "total_strings": 1,
      "similarity": 100,
      "attribution_entity": "eicar",
      "aliases": "EICAR test"
}
```

Свойства

Эта модель данных имеет следующие свойства.

Таблица 22. SimilarData свойства

Имя	Обязательный	Множественный	Тип значения	Описание
`md5`	Да	Нет	`string`	MD5-хеш аналогичного образца.
`size`	Да	Нет	`integer`	Размер выборки в байтах.
`matched_genotypes_count`	Да	Нет	`integer`	Количество генотипов, соответствующих проанализированному образцу.
`total_genotypes`	Да	Нет	`integer`	Общее количество генотипов в выборке.
`matched_strings_count`	Да	Нет	`integer`	Количество строк, соответствующих проанализированному образцу.
`total_strings`	Да	Нет	`integer`	Общее количество строк в сэмпле.
`similarity`	да	Нет	`integer`	Процент сходства с анализируемым образцом.
`attribution_entity`	Да	Нет	`string`	Имя объекта атрибуции, которому принадлежит образец.
`aliases`	Нет	Нет	`string`	Алиасы объекта атрибуции, которому принадлежит образец.

GenotypeData

Содержит информацию о генотипе в образце, который был сопоставлен с генотипами аналогичных образцов.

Пример

```
{
      "genotype": "0c91483bf75cab06bca6dbd41ff2a54e",
      "matched": 1,
      "used_by": [
        {
          "attribution_entity": "entity1",
          "matched": 1
        }
      ]
}
```

Свойства

Эта модель данных имеет следующие свойства.

Таблица 23. Свойства GeneData

Имя	Обязательный	Множественный	Тип значения	Описание
genotype	Да	Нет	string	Генотип в образце, который соответствовал генотипам аналогичных образцов.
matched	Да	Нет	integer	Количество известных выборок объектов атрибуции, имеющих этот генотип.
used_by	Да	Да	UsedByData (см. стр. 78)	Массив объектов атрибуции, которым принадлежат образцы с этим генотипом.

StringData

Содержит информацию о строке в образце, сопоставленной со строками из аналогичных образцов.

Пример

```
{
  "string": "ExampleString",
  "matched": 1,
  "used_by": [
    {
      "attribution_entity": "entity1",
      "matched": 1
    }
  ]
}
```

Свойства

Эта модель данных имеет следующие свойства.

Таблица 24. Свойства StringData

Имя	Обязательный	Множественный	Тип значения	Описание
`string`	Да	Нет	`string`	Строка в образце, соответствующая генотипам аналогичных образцов.
`matched`	Да	Нет	`integer`	Количество известных образцов объектов атрибуции, имеющих эту строку.
`used_by`	Да	Да	`UsedByData` (см. стр. 78)	Массив объектов атрибуции, которым принадлежат образцы с этой строкой.

ReportData

Содержит результаты анализа пробы.

Если была указана операция распаковки, ответ будет содержать массив элементов `ReportData`.

Пример

```
{
  "md5": "8ab5ae1feae8d3f83185288a34234bbd",
  "parent_md5": "5e7b97af0eeadcd5633395de5c53eae9"
  "extracted_path": "/example.zip/example.exe"
  "unpacking_status": 0
  "filename": "example.exe",
  "size": 245872,
  "top_5": [
    {
      "attribution_entity": "entity1",
      "similarity": 100
    }
  ],
  "matched_bad_genotypes": 1,
  "total_bad_genotypes": 1,
  "matched_bad_strings": 1,
  "total_bad_strings": 1,
  "result_code": 100,
  "similar_samples": [
    {
```

```
      "md5": "2fadca02bea0133991e2cff82211ac13",
      "size": 245876,
      "matched_genotypes_count": 1,
      "total_genotypes": 1,
      "matched_strings_count": 1,
      "total_strings": 1,
      "similarity": 100,
      "attribution_entity": "entity2",
      "aliases": "ENT2"
    }
  ],
  "matched_genotypes": [
    {
      "genotype": "cfadca02bc40133991e442b82311eff",
      "matched": 1,
      "used_by": [
        {
          "attribution_entity": "ENT2",
          "matched": 1
        }
      ]
    }
  ],
  "matched_strings": [
    {
      "string": "string",
      "matched": 1,
      "used_by": [
        {
          "attribution_entity": "ENT2",
          "matched": 1
        }
      ]
    }
  ]
}
```


Свойства

Эта модель данных имеет следующие свойства.

Таблица 25. Свойства ReportData

Имя	Обязательный	Множественный	Тип значения	Описание
`md5`	Да	Нет	`string`	MD5-хеш анализируемого файла.
`parent_md5`	Нет	Нет	`string`	MD5-хеш родительского файла анализируемого файла. Этот параметр используется для распакованных архивов.
`extracted_path`	Нет	Нет	`string`	Путь внутри родительского файла к анализируемому файлу. Этот параметр используется для распакованных архивов.

Имя	Обязательный	Множественный	Тип значения	Описание
`unpacking_status`	Да	Нет	`integer`	Состояние операции распаковки. Возможны следующие значения: • `0` Операция распаковки прошла успешно или не требовалась. • `1` Не удалось распаковать операцию. Произошла ошибка. • `2` Не все распакованные образцы были отправлены на анализ, так как был достигнут предел количества распакованных файлов.
`filename`	Да	Нет	`string`	Имя анализируемого файла.
`size`	Да	Нет	`integer`	Размер файла в байтах.
`top_5`	Да	Да	`Top5Data` (см. стр. 78)	Массив с пятью первыми объектами атрибуции сущностей, образцы которых наиболее похожи на анализируемую.

Имя	Обязательный	Множественный	Тип значения	Описание
`matched_bad_genotypes`	Да	Нет	`integer`	Соответствующие генотипы. Количество генотипов в анализируемой выборке, совпадающих с генотипами в аналогичных выборках.
`total_bad_genotypes`	Да	Нет	`integer`	Общие генотипы. Количество генотипов в анализируемой выборке, которые соответствуют выборкам известных объектов атрибуции.
`matched_bad_strings`	Да	Нет	`integer`	Соответствующие строки. Количество строк в анализируемой выборке, совпадающих со строками в аналогичных выборках.
`total_bad_strings`	Да	Нет	`integer`	Всего плохих строк. Общее количество неверных строк в проанализированной выборке, которые совпадают с выборками известных объектов атрибуции.

Имя	Обязательный	Множественный	Тип значения	Описание
result_code	Да	Нет	integer	Код результата анализа. Список кодов результатов см. В разделе Загрузка отчетов. (см. стр. 49) и интерпретация результатов анализа (см. стр. 42).
similar_samples	Да	Да	SimilarData (см. стр. 79)	Массив с похожими образцами объектов.
matched_genotypes	Да	Да	GenotypeData (см. стр. 80)	Массив объектов генотипов, соответствующих генотипам в выборке.
matched_strings	Да	Да	StringData (см. стр. 81)	Массив строковых объектов, соответствующих генотипам в выборке.

kaspersky

Как получить техническую поддержку

Если вы не можете найти решение вашей проблемы в документации, мы рекомендуем вам обратиться в службу технической поддержки.

Для получения технической поддержки обращайтесь по адресу ktlsupport@kaspersky.com.

«Лаборатория Касперского» предоставляет клиенту Техническую поддержку, которая включает решение проблем клиента, связанных с приобретенным продуктом. Kaspersky следит за тем, чтобы заказчик правильно использовал продукт в соответствии с его назначением и в соответствии с документацией и техническими характеристиками.

Заказчик предоставляет максимально подробную информацию, чтобы помочь Службе технической поддержки «Лаборатории Касперского» решить проблему или позволить «Лаборатории Касперского» исправить любые проблемы в продукте или продолжить разработку продукта в соответствии с требованиями «Лаборатории Касперского».

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле docs / legal_notices.txt в дистрибутиве Kaspersky Threat Attribution Engine.

kaspersky

О предоставлении данных

В этом разделе описывается процесс предоставления данных.

«Лаборатория Касперкого» защищает любую полученную информацию в соответствии с законодательством и применимыми правилами «Лаборатории Касперкого». Данные передаются по защищенному каналу.

Данные, предоставляемые в инфраструктуру «Лаборатории Касперкого»

Во время работы Kaspersky Threat Attribution Engine пользовательские данные не передаются в инфраструктуру «Лаборатории Касперкого».

Данные, хранящиеся в Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine хранит данные, предоставленные пользователями для ознакомления с продуктом.

Все пользовательские данные хранятся в пользовательской инфраструктуре. Никакие данные в инфраструктуру «Лаборатории Касперкого» не передаются.

Данные, хранящиеся в файлах журнала

Расположение: Локальный сервер Kaspersky Threat Attribution Engine.

Место хранения: 30 дней или до 1 гигабайта (ГБ).

Контроль доступа: Безопасность файловой системы Linux.

В файлах журнала хранятся следующие данные:

- Фрагменты файлов и метаданные загруженного отчета. Информация метаданных - это имена файлов, пути к файлам, размер файла и информация об объектах атрибуции.
- Фрагменты файлов и метаданные анализа и образцы запросов на вложения. Метаданные содержат информацию об объектах атрибуции, именах файлов и размере файла.
- Данные ответа результата анализа.

Данные, хранящиеся в базе данных MySQL

Расположение: Локальный сервер Kaspersky Threat Attribution Engine.

Срок хранения: бесконечный.

Контроль доступа: Безопасность MySQL.

В базе данных MySQL хранятся следующие данные:

- Идентификатор сеанса пользователя
- Имя пользователя созданной учетной записи пользователя
- Логин созданной учетной записи пользователя
- Хеш пароля созданной учетной записи пользователя
- Фрагменты файлов (генотипы и строки)
- Метаданные файла (имена файлов, пути к файлам)

Данные, хранящиеся в домашней директории пользователя

В домашней директории пользователя хранится флаг принятия EULA

Данные, хранящиеся во временном хранилище

Расположение: Локальный сервер Kaspersky Threat Attribution Engine

Срок хранения: до окончания обработки задания

Контроль доступа: Безопасность файловой системы Linux

Во временном хранилище хранятся следующие данные:

- Файлы, отправленные на анализ и прикрепление образцов пользователями
- Фрагменты файлов (генотипы и строки)

kaspersky

Дорогой пользователь,

Спасибо, что выбрали «Лабораторию Касперкого» в качестве поставщика программного обеспечения для обеспечения безопасности. Мы надеемся, что этот документ поможет вам использовать наш продукт.

Дата редакции документа: 19.01.2021

https://www.kaspersky.com https://help.kaspersky.com https://support.kaspersky.com

О «Лаборатории Касперкого»: (https://www.kaspersky.com/about/company)

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью соответствующих владельцев.