АО «Система Безопасных Коммуникаций»

123458, г. Москва, Строгино, ул. Маршала Прошлякова, д. 30, офис 307, ком. 1

+7 495 789-04-56

info@communigatepro.ru

Руководство администратора Внешнего помощника CGP-KAV версии 1.1.3

В документе описано, как устанавливать, настраивать и запускать Внешний помощник CGP-KAV для CommuniGate Pro актуальной версии 1.1.3, необходимый для проверки электронных писем с помощью Анти-Вируса Касперского. В электронные письма будут добавлены заголовки почтовых сообщений с результатами проверок. Это позволит автоматически фильтровать электронные письма с помощью правил.

Сокращения

- KAV: Анти-Вирус Касперского
- KSN: Kaspersky Security Network
- CGPro: CommuniGate Pro

Требования

CommuniGate Pro: 6.3.39 и новее

Операционная система: Linux x86_64

Лицензии

Убедитесь, что лицензии для внешнего помощника CGP-KAV добавлены в CGPro. Для этого откройте раздел интерфейса администратора CGPro `Главное → Лицензия` Если лицензионные ключи помощников CGP-KAV добавлены, в списке будут записи, содержащие “Kaspersky AnviVirus”.

Доступ к внешней сети

Технологиям Kaspersky необходим доступ к Kaspersky Security Network для обновления базы данных вирусных сигнатур. Некоторые функции сканирования, используемые для повышения точности, могут требовать отправки данных в Kaspersky Security Network. Вам необходимо открыть сетевой доступ по протоколам HTTP и HTTPS (80-TCP, 443-TCP) на следующие адреса:

- `*.kaspersky-labs.com`
- `*.kaspersky.com`

Установка Помощника

Установка из дистрибутива

Скачайте последнюю версию пакета для вашей системы

```
# cd cgpro_home
# sudo tar xf path/to/CGP-KAV-Linux-amd64_vX.Y.Z.tar.bz2
# sudo chown -R root:mail cgpro_home/CGP-KAV
```

где `cgpro_home` - это путь к директории установленного CGPro.

Настройка Помощника

Чтобы добавить внешнего помощника CGP-KAV, в интерфейсе администрирования CGPro перейдите в `Помощники`. Создайте и включите новый помощник в разделе `Фильтрация данных`, заполните параметры помощника (пример):

Параметр	**Значение**
Имя	AntiVirus
Уровень журнала	Все
Путь к Программе	CGP-KAV/CGP-kAV
Тайм-аут	2мин
Авторестарт	15сек

Настройка правил

Создадим правило для сканирования всех писем, направляемые через модуль LOCAL, который доставляет письма в почтовые ящики пользователей. Такие настройки означают, что любое письмо будет направлено во Внешний помощник CGP-KAV.

Перейдите в раздел [Автоматические Правила]

Добавьте новое правило с названием `AntiVirus` и нажмите `Изменить`. Установите в правиле следующие параметры :

Данные	**Операция**	**Параметр**
Любой Маршрут	равно	LOCAL(*

Действие	**Параметр**
Внешний Фильтр	`AntiVirus`

Включение Внешнего помощника

В интерфейсе администрирования CGPro перейдите в раздел [Помощники] и выберите для Фильтра данных `AntiVirus` со значения `Выключено` на `Включено`.

Выключение Внешнего помощника

В интерфейсе администрирования CGPro перейдите в раздел [Помощники] и измените для Фильтра данных `AntiVirus` со значения `Включено` на `Выключено`.

> Обратите внимание, что KAV нужно порядка 15-30 секунд на корректное завершение работы.

Утилита диагностики

Убедиться, что помощник CGP-KAV работает так, как ожидается, с помощью утилиты диагностики. Утилита диагностики может быть также использована в случае проблем с запуском внешнего помощника через CGPro. Пожалуйста, обратитесь к разделу Отладка внешнего помощника CGP-KAV для получения более подробной информации.

```
# cd cgpro_home/CGP-KAV
# sudo ./diagnose
```

Настройка Внешнего помощника CGP-KAV

Этот раздел описывает параметры конфигурирования, которые находятся в `cgpro_home/CGP-KAV/kav.conf`

Конфигурационный файл регистрозависимый.

- Основные настройки (блок `[main]`):
    - Путь к инсталляции CGPro:

      ```
      cgpro_home = /var/CommuniGate
      ```

    - Политика отказов позволяет определить, как будет действовать Внешний помощник в случае сбоев при вызове KAV. Если политика фильтрации определена как отклонение сообщения, любая ошибка сканирования заставит Внешнего помощника отложить сообщение в очереди CGPro. Любая другая ошибка, кроме ключевого слова `reject`, будет указывать помощнику на то, что письмо должно быть доставлено (политика `pass`). В

этом случае к письму добавляется заголовок ошибки (`X-KAV-Error`). Параметр политики отказа :

```
failure_policy = reject|pass
```

- Количество потоков, обрабатывающих очередь сообщений.

```
worker_threads = 4
```

- Стартовая задержка позволяет отсрочить запуск Внешнего помощника, чтобы убедиться, что CGPro доступен для получения лицензий :

```
delay_start = 0
```

- Адрес и порт, на котором запускается KAV SDK

```
ConnectionString = localhost:7776
```

- Настройки антивируса (блок [antivirus]).

  Относятся к настройкам KAV и перезаписывают значения в файле `cgpro_home/CGP-KAV/KAV/etc/kavhttpd.xml`

  Вы можете добавить собственные заголовки результатов в электронные письма после того, как они были успешно просканированы KAV, например:

  - `KAV_Header_Status = X-KAV-Status`
  - `KAV_Header_Extended = X-KAV-Extended`
  - `KAV_Header_Error = X-KAV-Error`

  Заголовок `KAV_Header_Extended` будет содержать идентификатор вируса в случае его обнаружения. Подробности см. в разделе Заголовки результатов сканирования.

  - Время в секундах, по истечении которого внешний помощник будет проверять наличие обновлений в базе вирусных сигнатур KAV перед сканированием нового сообщения электронной почты. Значение по умолчанию - 360 минут (6 часов):

    ```
    UpdatePeriodMinutes = 360
    ```

  - Количество процессов и потоков сканера, которые будут запущены службой KAV при запуске внешнего помощника. Более подробная информация и советы по настройке этих параметров приведены в разделе Настройки производительности. Значения по умолчанию:

`ScannersCount = 2` // ограничивается системой (ulimit -u) `ThreadsCount = 2` // максимум 32

- Таймаут сессии (SessionTimeout) в миллисекундах, по истечении которого сканирование будет прервано и выдаст ошибку таймаута. В зависимости от политики отказа (reject или pass) в главном разделе конфигурации, письмо будет выпущено с заголовком ошибки или отложено для другой попытки. По умолчанию для сканирования сообщений установлено значение 10 000 миллисекунд (10 секунд):

  `SessionTimeout = 10000`

  Время, необходимое для сканирования письма, зависит от вычислительных возможностей вашего оборудования, размера писем и загруженности системы в момент вызова сканирования. Вы можете настроить этот параметр в зависимости от типа SMTP-потока, который вы хотите направить в KAV для сканирования.

Отладка внешнего помощника CGP-KAV

Для того чтобы внешний помощник мог вести полные журналы, необходимо активировать запись полных журналов в модуле сбора сообщений: [Установка почты в очередь] → Уровень журнала : Всё

Чтобы отладить внутренние функции внешнего помощника, вы можете активировать режим `verbose` для различных модулей в секции [debug] конфигурационного файла `kav.conf` :

```
DebugExternal = 0 // выводит инофрмацию об ограничениях лицензии (значения 0,1)
DebugFilterDaemon = 0 // выводит информацию о взаимодейтсвии с KAS (значения 0,1)
DebugThreading = 0  // отчёты о работе потоков (значения 0,1)
DebugConfig = 0 // выводит актуальные конфиги помощника (значения 0,1)
DebugCGateInput = 0 // выводит запросы, приходящие от CGate (значения 0,1)
```

Заголовки результатов сканирования

Заголовки, добавляемых в письма, проверяемые внешним помощником CGP-KAV:

Угроза	**Заголовок**
Не обнаружена	X-KAV-Status: CLEAN
Обнаружена	X-KAV-Status: DETECT

Угроза	Заголовок
Обнаружена	X-KAV-Extended <virus_id>

Ошибка `X-KAV-Error : <message>` добавляется к письму при возникновении ошибки.

Расширенные настройки

Позволяют настроить сетевой прокси-доступ для сервисов KAV и получить доступ к тонкой настройке KAV.

Пара опций в этих файлах управляется самим внешним помощником. Не изменяйте эти опции, иначе это может нарушить работу механизма перезаписи файлов конфигурации при следующем перезапуске внешнего помощника. Опции, которые будут переписаны, всегда устанавливаются в 0 в конфигурационных файлах шаблона, их легко определить.

Файлы конфигурации KAV Engine: `cgpro_home/CGP-KAV/KAV/kavhttpd/etc/kavhttpd.xml`
Прим. Параметры kav.conf из раздела [antivirus] перезаписывают соответствующие параметры файла `kavhttpd.xml`

Настройки сетевых прокси сканера

Отредактируйте файл конфигурации сканера KAV и измените этот раздел в соответствии с параметрами вашего сетевого прокси-сервера:

```
<UseHTTPProxy>0</UseHTTPProxy> <!-- Specifies whether KAV HTTPD uses proxy when maki
KSN: 0 (not used) or 1 (used) -->
<HTTPProxy>
    <url></url> <!-- Address of the proxy -->
    <port></port> <!-- Port of the proxy -->
    <user></user> <!-- User name for the proxy authentication -->
    <pass></pass> <!-- Password for the proxy authentication -->
</HTTPProxy>
```

Настройки сетевых proxy сервиса обновления

Задаются в разделе `ProxySettings` файла `cgpro_home/CGP-KAV/KAV/kavhttpd/etc/kavhttpd.xml`

```
<ProxySettings>
    <UseProxy>0</UseProxy>
    <ProxyUrl>proxy.somehost.com</ProxyUrl>
```

```
    <ProxyPort>80</ProxyPort>
    <ProxyLogin>ProxyUser</ProxyLogin>
    <ProxyPassword>ExamplePassword</ProxyPassword>
    <ProxyRequiresAuthorization>0</ProxyRequiresAuthorization>
    <NtlmAuthorization>1</NtlmAuthorization>
</ProxySettings>
```

Настройки KAV Scan Engine

Определяются в разделе `ServerSettings` файла: `cgpro_home/CGP-KAV/KAV/kavhttpd/etc/kavhttpd/kavhttpd.xml`

```
<ServerSettings>
    <Flags>KAV_SHT_ENGINE_KLAV | KAV_SHT_ENGINE_KLAVEMU | KAV_SHT_ENGINE_WMUF</Flags
</ServerSettings>
```

`Flags` указывает параметры инициализации Kaspersky Scan Engine. Параметры инициализации определяются комбинацией флагов, разделенных вертикальными чертами (|).

Флаг	**Описание**
KAV_SHT_ENGINE_KLAV	Разрешить загрузку нового основного антивирусного движка (KLAV).
KAV_SHT_ENGINE_KLAVEMU	Разрешить загрузку продвинутого эвристического антивирусного движка (эмулятора KLAV).
KAV_SHT_ENGINE_WMUF	Включить компонент фильтрации WMUF. Компонент использует базу данных WMUF.
KAV_SHT_ENGINE_KSN	Включить использование Cloud Protection для проверки репутации файлов и URL-адресов.

> Обратите внимание, что для включения проверки репутации URL-адресов необходимо включить флаги `KAV_SHT_ENGINE_WMUF` и `KAV_SHT_ENGINE_KSN`.

Для включения проверки репутации файлов достаточно флага `KAV_SHT_ENGINE_KSN`.

> Обратите внимание, что, установив флаг `KAV_SHT_ENGINE_KSN`, вы соглашаетесь на передачу файла с данными в "Лабораторию Касперского".

Настройки KAV SDK

Указывает настройки сканирования для KAV SDK, который является частью Kaspersky Scan Engine.

```
<KAVScanningSettings>
    <Flags>KAV_O_M_PACKED | KAV_O_M_ARCHIVED | KAV_O_M_MAILPLAIN | KAV_O_M_COMPOSITE
        KAV_O_M_HEURISTIC_LEVEL_DETAIL</Flags>
    <Mode>KAV_SKIP</Mode>
</KAVScanningSettings>
```

- KAV_O_M_PACKED

  Включение сканирования сжатых исполняемых файлов

- KAV_O_M_ARCHIVED

  Сканирование заархивированных файлов включено. KAV Engine автоматически добавит флаг `KAV_O_M_PACKED` к маске сканирования, если вы установили флаг `KAV_O_M_ARCHIVED` . Включение сканирования архивных файлов также автоматически включает сканирование упакованных исполняемых файлов, но не наоборот. |

- KAV_O_M_BACKUP Включение сохранения копий зараженных объектов в резервном хранилище. Копии сохраняются до того, как оригинальные объекты будут вылечены или удалены.

  При обнаружении составного зараженного объекта (например, архива, упакованного объекта, сообщения электронной почты, базы данных электронной почты) в резервное хранилище сохраняется копия всего объекта, а не только его зараженной части.

  Когда одна из этих функций вызывается с этим флагом и обнаруживает зараженный объект, она автоматически помещает оригинальную копию зараженного файла в резервное хранилище, и только после этого выполняются дальнейшие операции, такие как лечение или удаление. Операции соответствуют выбранному режиму очистки. |

- KAV_O_M_MAILPLAIN Включение сканирования сообщений электронной почты.

  Установка этого параметра сканирования обеспечивает поддержку следующих форматов файлов обычных сообщений электронной почты:

  - Текстовые сообщения в формате RFC 822
  - Файлы сообщений Microsoft Outlook (MSG)
  - Любые файлы, закодированные с использованием текстовых кодировок UUE/XXE/base64, например архивы UUE.

- KAV_O_M_HEURISTIC_LEVEL_SHALLOW Включение расширенного эвристического анализатора кода. Этот анализатор основан на улучшенной технологии обнаружения; уровень сканирования будет более низким.

  Уровень детализации продвинутого эвристического анализатора обеспечивает баланс между качеством сканирования и потреблением ресурсов операционной системы, а также продолжительностью сканирования. Чем выше уровень продвинутой эвристики, тем больше системных ресурсов требуется, и тем дольше длится сканирование.

- KAV_O_M_HEURISTIC_LEVEL_MEDIUM Включение расширенного эвристического анализатора кода. Этот анализатор основан на улучшенной технологии обнаружения; уровень сканирования будет средним.

  Уровень детализации продвинутого эвристического анализатора обеспечивает баланс между качеством сканирования и потреблением ресурсов операционной системы, а также продолжительностью сканирования. Чем выше уровень продвинутой эвристики, тем больше системных ресурсов требуется, и тем дольше длится сканирование.

- KAV_O_M_HEURISTIC_LEVEL_DETAIL Включение расширенного эвристического анализатора кода. Этот анализатор основан на улучшенной технологии обнаружения; уровень сканирования будет более детальным.

  Уровень детализации продвинутого эвристического анализатора обеспечивает баланс между качеством сканирования и потреблением ресурсов операционной системы, а также продолжительностью сканирования. Чем выше уровень продвинутой эвристики, тем больше системных ресурсов требуется, и тем дольше длится сканирование.

- KAV_O_M_HEURISTIC_LEVEL_MAXIMUM Этот флаг позволяет включает режим тщательного эвристического анализа в KAV Engine, который дает возможность вашему приложению получить еще более сложную эвристическую эмуляцию файлов и других объектов, которые вы сканируете.

  Включение этого режима сканирования обеспечивает более высокую эффективность обнаружения за счет максимально возможной глубины эвристической эмуляции.

  Чрезвычайно тщательная эвристическая эмуляция обеспечивается за счет снижения скорости сканирования. Использование этого режима сканирования может привести к значительному снижению скорости сканирования.

- KAV_O_M_URL Обеспечивает сканирование каждого запрашиваемого адреса URL.

Когда веб-страница открывается в браузере, ее веб-адрес проверяется по базе данных Web Malicious Url Filtering (WMUF). Сюда входят веб-адреса, запрашиваемые из приложения браузера, и URL-адреса веб-страниц, запрашиваемые в открываемой веб-странице. Если при использовании открывается веб-страница, содержащая скрипт или iFrame, запрашивающий другой веб-адрес, по базе WMUF проверяется как адрес исходной веб-страницы, так и встроенные URL-адреса.

- KAV_O_M_COMPOSITE_SCAN_KSN Позволяет проверять многократно упакованные файлы с помощью облачного сервиса Kaspersky.

  Многопакетные файлы, например архивные файлы или самораспаковывающиеся архивы, упакованные несколько раз, или файлы со встроенными объектами OLE могут быть проверены в облачном сервисе Kaspersky KSN.

  Если KAV обнаруживает объект, сканируемый по локальной базе данных, KAV повторно сканирует его в облаке, даже если флаг KAV_O_M_COMPOSITE_SCAN_KSN выключен. Повторное сканирование объекта в облачном сервисе обеспечивает защиту от ложных обнаружений.

  Когда статус сканирования объекта с помощью локальной базы данных равен `KAV_S_R_CLEAN` , KAV проверяет, был ли использован флаг `KAV_O_M_COMPOSITE_SCAN_KSN` . Если флаг не использовался, проверки в облаке не выполняются. Если флаг был использован, KAV SDK повторно сканирует объект с помощью KSN.

  Этот флаг должен использоваться с любой комбинацией следующих флагов: - KAV_O_M_PACKED - KAV_O_M_ARCHIVED - KAV_O_M_MAILBASES - KAV_O_M_MAILPLAIN

  Если ни один из перечисленных флагов не указан, KAV_O_M_COMPOSITE_SCAN_KSN игнорируется.

  Обратите внимание, что при включении `KAV_O_M_COMPOSITE_SCAN_KSN` и `KAV_SHT_ENGINE_KSN` , вы соглашаетесь на передачу файла данных в Лабораторию Касперского.

- KAV_O_M_RECOGNIZE_FILE_FORMAT Включить распознавание формата файлов.

- KAV_O_M_RECOGNIZE_ NESTED_FILES_FORMAT Включить распознавание формата для вложенных файлов.

Доступные режимы инициализации KAV Engine

```
<Mode>KAV_SKIP</Mode>
```

KAV_SKIP Если при сканировании объекта обнаружено вредоносное ПО, KAV Engine не будет предпринимать никаких попыток лечения или удаления вредоносного объекта. Текущая задача сканирования будет пропущена.

Обновление лицензионных ключей KAS

Периодически внутренние ключи движков KAV нуждаются в обновлении. В этом случае АО «СБК» предоставит вам ключи и инструкции по их обновлению.

Настройки производительности

Рекомендации Лаборатории Касперского по настройке KAV

Для повышения производительности движка KAV рекомендуется установить значения `ThreadsCount` и `ScannersCount` равными количеству логических ядер в системе. Производительность снизится, если вы добавите больше потоков или сканеров, чем доступно логических ядер. В случае если оба параметра имеют разные значения, KAV Engine будет использовать минимальное из них.

Согласно статистике Лаборатории Касперского в 2018 году, если вы сканируете письма размером менее 5 МБ, вы покрываете 98% вредоносных программ, присутствующих в почтовом потоке.

Чтобы повысить производительность, можно исключить объекты, отфильтровав определенные типы файлов. Поскольку некоторые типы файлов не являются вредоносными по своей сути, есть возможность разрешить определенным типам файлов обходить механизм сканирования на основании их расширения.

Существует также ряд объектов с низким уровнем опасности, например видеопотоки, музыкальные файлы и изображения. Возможно, будет полезно избежать сканирования таких файлов.

По информации специалистов Лаборатории Касперского, было обнаружено несколько уязвимостей, например, в различных графических просмотрщиках и редакторах, обрабатывающих изображения, поэтому есть шанс, что вредоносное изображение воспользуется существующей уязвимостью. Однако, на данный момент было найдено всего несколько PoC-образцов подобных атак, и реальное заражение системы с помощью вредоносных изображений или видеофайлов - очень редкий случай по сравнению с другими типами объектов, используемых вредоносным ПО для распространения через Интернет.

Эти типы содержимого можно исключить:

- text/plain;
- text/css;
- image/bmp;
- image/gif;
- image/png;
- image/jpg;
- audio/mp3;

Аналитики Лаборатории Касперского настоятельно рекомендуют сканирование следующих типов содержимого:

- text/html
- application/octet-stream
- application/x-javascript
- application/x-shockwave-flash

> Примечание: Предыдущие правила могут использоваться для обнаружения и маркировки писем по типу содержимого, чтобы иметь возможность исключить/включить их в правило, вызывающее внешний помощник CGP-KAV.