Внешний помощник Kaspersky для CommuniGate Pro 6.3

Руководство пользователя

Версия продукта :	1.0.0
Версия документации :	1.0
Дата :	01.12.2023

Содержание

Предисловие

В этом документе описано, как устанавливать, настраивать и запускать Внешний помощник Kaspersky для CommuniGate Pro, необходимый для проверки электронных писем с помощью Анти-Вируса Касперского и Анти-Спама Касперского. В электронные письма будут добавлены SMTP-заголовки с результатами проверок. Это позволит автоматически фильтровать электронные письма с помощью SMTP-правил CommuniGate Pro.

Требования

CommuniGate Pro: 6.3.31 и новее

GNU/Linux: встраиваемые продукты Лаборатории Касперского совместимы с glibc-2.11

Примечания

Технологиям Kaspersky необходим доступ к Kaspersky Security Network для обновления базы данных определений антиспама и 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 хосты:

*.kaspersky-labs.com

*.kaspersky.com

Сокращения

KAS: Анти-Спам Касперского

KAV: Анти-Вирус Касперского

KSN: Kaspersky Security Network

CGPro: CommuniGate Pro

Установка Помощника Kaspersky

В этом разделе описано, как устанавливать Внешний помощник Kaspersky.

cgpro_home - это путь к директории установленного CGPro.

Установка из дистрибутива

Скачайте последнюю версию пакета для вашей системы по адресу:

https://www.communigatepro.ru/pub/plugins/Kaspersky/

```
# cd cgpro_home
# sudo tar xf path/to/Kaspersky-1.0.x-Linux-<platform>.tar.bz2
# sudo chown -R root:mail cgpro_home/Kaspersky
```

CommuniGate Pro

Чтобы внешний помощник Kaspersky обрабатывал почту, необходимо объявить этот новый помощник и создать SMTP-правило для вызова помощника на основе почтового потока.

Настройка внешнего помощника

Чтобы добавить внешнего помощника Kaspersky, в интерфейсе администрирования CGPro перейдите в
Установки → Общее → Помощники

Создайте новый помощник в разделе Фильтрация данных:

Выключено	Kaspersky		
Уровень журнала	Все	**Путь к Программе**	Kaspersky/Kaspersky
Тайм-аут	2мин	**Авторестарт**	15сек

Настройка SMTP-правил

В данном примере показано, как сканировать все письма, направляемые через модуль LOCAL, который будет доставлять письма в почтовые ящики пользователей. Такие настройки означают, что любое письмо, отправленное даже от вас самих на ваш собственный почтовый ящик, будет направлено во Внешний помощник Kaspersky.

Перейдите в раздел Установки → Почта → Правила

Добавьте новое правило с названием Kaspersky и нажмите Изменить

Добавьте в правило следующие параметры :

Данные	**Операция**	**Параметр**
Любой Маршрут	равно	LOCAL(*
Действие		**Параметр**
Внешний Фильтр		Kaspersky

Лицензии

Убедитесь, что лицензии для внешнего помощника Kaspersky добавлены в CGPro. Для этого откройте раздел интерфейса администратора CGPro `Главное → Лицензия`

Если лицензионные ключи помощников Kaspersky добавлены, в списке будут записи, содержащие “`Kaspersky AnviVirus`” или “`Kaspersky AntiSpam`”.

Запуск Внешнего помощника Kaspersky

Утилита диагностики

Теперь можно убедиться, что движки KAS/KAV работают в вашей системе так, как ожидается, с помощью утилиты диагностики. Это не является обязательным перед запуском помощника. Она может быть использована в случае проблем с запуском внешнего помощника через CGPro. Пожалуйста, обратитесь к разделу Отладка внешнего помощника Kaspersky для получения более подробной информации.

```
# cd cgpro_home
# sudo ./Kaspersky/diagnose
```

Включение Внешнего помощника

В интерфейсе администрирования CGPro перейдите в раздел `Настройки → Общее → Помощники` и измените для Фильтра данных Kaspersky значение Выключено на Включено.

Настройка Внешнего помощника Kaspersky

Этот раздел описывает параметры конфигурирования, которые находятся в *`cgpro_home`*`/Kaspersky/kaspersky.conf`

Конфигурационный файл регистрозависимый.

Основные настройки

Основные настройки определены в блоке **`[main]`**.

Необходимо указать помощнику путь к инсталляции CGPro :

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

Указать настройки подключения к CGPro для загрузки лицензий :

```
# http|https
cgpro_httpa_scheme = https
cgpro_httpa_ip = 127.0.0.1
cgpro_httpa_port = 9010
```

Если вы используете внешний помощник Kaspersky и для Анти-Спама, и для Анти-Вируса, можно выбрать движок, вызываемый первым :

```
filtering_policy = KAS_First|KAV_First
```

Политика отказов позволяет определить, как будет действовать Внешний помощник в случае сбоев при вызове движков KAV/KAS. 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-KAS-Error или X-KAV-Error). Параметр политики отказа :

failure_policy = reject|pass

Рабочие потоки позволяют настроить количество потоков, обрабатывающих очередь сообщений движками KAV/KAS.

worker_threads = 4

Для просмотра лицензий CGPro у учётной записи пользователя должны быть соответствующие права :

license_user = *login // Права → Разрешено всё*
license_pwd = *password*

В случае проблем с движками KAV/KAS вы можете включить функцию автоперезапуска на основе обнаружения пороговых сбоев. По умолчанию любое письмо, которое будет отправлено на сканирование 5 раз, потребует перезапуска движков KAV/KAS перед новым отправлением на сканирование:

auto_restart = 0|1
fail_restart_threshold = 5

Следующая настройка позволяет отсрочить запуск Внешнего помощника, чтобы убедиться, что CGPro доступен для получения лицензий :

delay_start = 0

Настройка отчётов

Настройка отчётов определена в разделе **[reporting]**.

Вы можете включить/выключить функцию создания отчётов :
enable = 0|1

Настройте ip/порт, чтобы Внешний помощник мог запускать WebUI для создания отчетов :
reporting_ip = 127.0.0.1
reporting_port = 8080

Для доступа к отчётам требуется аутентификация :
reporting_user = someuser
reporting_pwd = somepass

В отчете есть временная шкала, для которой можно настроить период хранения данных. Данные консолидируются по временным меткам с разрешением в минуту. По умолчанию сохраняются данные за 24 часа (т.е. 1440 минут):
reporting_timeline = 1440

Настройки Anti-Virus

Настройки антивируса определяются в разделе **[antivirus]**.

Вы можете задать период времени 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 - 21600 секунд (6 часов):

```
KAV_update_period = 21600
```

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

```
KAV_Header_Status = X-KAV-Status
```

```
KAV_Header_Extended = X-KAV-Extended
```

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

Вы можете настроить 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
```

Вы можете задать 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.

Настройки Anti-Spam

Настройки антиспама задаются в разделе **[antispam]**.

Вы можете задать период времени в секундах, по истечении которого внешний помощник будет проверять наличие обновлений службы KAS. Для достижения максимальной точности при использовании этой технологии защиты от спама рекомендуется проверять обновления с интервалом от 1 до 5 минут. Значение по умолчанию - 1 мин:

```
UpdateInterval = 1min
```

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

```
KAS_Header_Status = X-KAS-Status
```

```
KAS_Header_Level = X-KAS-Level
```

```
KAS_Header_Method = X-KAS-Method
```

Смотрите подробности в разделе Заголовки результатов сканирования.

Вы можете задать таймаут сканирования (ScanningTimeout) в секундах, по истечении которого сканирование будет прервано и выдаст ошибку таймаута. В зависимости от политики отказа (reject или pass) в основном разделе конфигурации, письмо будет выпущено с заголовком ошибки или отложено для другой попытки. Значение по умолчанию для сканирования сообщений составляет 2 секунды:

```
ScanningTimeout = 2sec
```

Вы можете включить/отключить функции KAS, используемые для оценки

электронной почты в соответствии с антиспамовыми детекторами:

```
UseHeuristic = 1 // Проверка текстов сообщений с помощью
лингвистического анализа

UseDMARC = 1 // Использовать метод обнаружения спама DMARC
UseLists = 1 // Использовать списки SURBL и DNSBL
UseAntiPhishing = 1 // Использовать антифишинговое обнаружение спама
UseGrahicalAnalysys = 1 // Использовать технологию обнаружения спама с
графическим распознаванием (GSG)
UseObsceneFiltration = 1 // Анализировать сообщения на предмет нецензурной
лексики. Такие сообщения помечаются специальным служебным заголовком
# Следующие опции позволяют передавать данные в Kaspersky Security Network
UseDNSHeuristic = 0 // Использовать обнаружение спама на основе DNS
UseCloud = 0 // Обнаружение спама на основе облачных технологий (UDS,
SURBL, URL Reputation)
UseEASUS = 0 // Использование Enforced Anti-Spam Updates Service
(EASUS)
UseReputationFiltering = 0 // Use Reputation Filtering spam detection
```

Настройки отладки

Настройки для отладки находятся под заголовком **[debug]**.

Прочтите секцию Отладка внешнего помощника Kaspersky чтобы включить сохранение журналов внешнего помощника в журналах CGPro и узнать больше о параметрах в разделе **[debug]**.

Заголовки результатов сканирования

В этом разделе представлен обзор заголовков, добавляемых в письма, проверяемые внешним помощником Kaspersky.

Kaspersky Anti-Virus Engine

Угроза не обнаружена

X-KAV-Status: CLEAN добавляется в просканированное письмо при отсутствии угрозы.

Угроза обнаружена

X-KAV-Status: DETECT добавляется в сканируемое письмо при обнаружении угрозы

X-KAV-Extended: <virus_id> добавляется в сканируемое письмо при обнаружении угрозы

Ошибка

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

Kaspersky Anti-Spam Engine

Спам не обнаружен

X-KAS-Status : KAS_STATUS_NOT_SPAM

X-KAS-Level : [] // рейтинг по шкале от 0 до 100, каждый X означает 10. В этом примере - 0.

X-KAS-Method: none

Спам обнаружен

X-KAS-Status : KAS_STATUS_SPAM

X-KAS-Level : [XXX] // рейтинг по шкале от 0 до 100, каждый X означает 10. В этом примере - 0.

X-KAS-Method: <*method id*> // метод, используемый для оценки письма

Список статусов KAS

Список статусов, которые KAS Engine может присвоить письму, приведен ниже:

KAS_STATUS_NOT_SPAM

KAS_STATUS_ERROR

KAS_STATUS_SPAM

KAS_STATUS_PROBABLE

KAS_STATUS_AUTO_RESPONDER

KAS_STATUS_BLACKLISTED

KAS_STATUS_TRUSTED_SOURCE

KAS_STATUS_MASS_MAIL

KAS_STATUS_QUARANTINED

Ошибка

X-KAS-Error : <message> добавляется к письму при возникновении ошибки.

Расширенные настройки

Расширенные настройки позволяют настроить сетевой прокси-доступ для сервисов KAV/KAS и получить доступ к тонкой настройке движков KAV/KAS.

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.

Kaspersky Anti-Virus Engine

Файлы конфигурации KAV Engine:

cgpro_home/Kaspersky/KAV/kavhttpd/etc/kavhttpd/kavhttpd.xml.template (scanner)

cgpro_home/Kaspersky/KAV/updater/etc/settings.xml (updater)

Настройки сетевых proxy 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 making requests to 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

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

```
<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 Scanner Engine

Файл, который необходимо отредактировать, чтобы изменить конфигурацию KAV engine:

cgpro_home/Kaspersky/KAV/kavhttpd/etc/kavhttpd/kavhttpd.xml.template

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

Подробнее о доступных флагах инициализации сервиса KAV:

KAV_SHT_ENGINE_KLAV	Битовый флаг, разрешающий загрузку нового основного антивирусного движка (KLAV).
KAV_SHT_ENGINE_KLAVEMU	Битовый флаг, разрешающий загрузку продвинутого эвристического антивирусного движка (эмулятора KLAV). Этот флаг следует установить, если вы собираетесь использовать расширенный эвристический режим сканирования.
KAV_SHT_ENGINE_WMUF	Включение компонента фильтрации WMUF. Компонент использует базу данных WMUF.
KAV_SHT_ENGINE_KSN	Включение использования Cloud Protection для проверки репутации файлов и URL-адресов. Обратите внимание, что для включения проверки репутации URL-адресов необходимо установить флаги должны быть установлены 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".

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

Информация о возможных параметрах инициализации KAV Engine:

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	Сканирование сообщений электронной почты включено. 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 включить 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:

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.

Kaspersky Anti-Spam Engine

Файл, который необходимо отредактировать, чтобы получить доступ к конфигурации движка KAS:

cgpro_home/Kaspersky/KAS/etc/kassdk_http_server.cfg.template

Настройки сетевых proxy

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

```
<ProxySettings>
  <Host></Host>
  <Port></Port>
  <User></User>
  <Pass></Pass>
  <AuthType>NTLM|BASIC|AUTO</AuthType>
</ProxySettings>
```

Обновление лицензионных ключей Kaspersky

Может оказаться, что внутренние ключи движков KAV/KAS нуждаются в обновлении. В этом случае АО «СБК» предоставит вам ключи, которые необходимо скопировать в директории cgpro_home/Kaspersky/update/KAV и/или cgpro_home/Kaspersky/update/KAS.

Чтобы применить новые ключи, вам нужно запустить следующую команду:

```
# cd cgpro_home/Kaspersky/update
# sudo ./deploy
```

Исполняемый файл deploy можно запускать и при работающем внешнем помощнике. Новые ключи будут использованы движками KAV/KAS при следующем перезапуске внешнего помощника.

Настройки производительности

Рекомендации Лаборатории Касперского по настройке KAS/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 для администраторов CGPro: Внешний помощник Kaspersky будет проверять любое письмо, отправленное на обработку CGPro. Правило SMTP, вызывающее помощника, отвечает за выбор SMTP-потока, направляемого помощнику. Предыдущие фильтры могут использоваться для обнаружения и маркировки писем по типу содержимого, чтобы иметь возможность исключить/включить их в SMTP-правило, вызывающее внешний помощник Kaspersky.

Установка в очередь CGPro и рабочие потоки внешнего помощника

Теоретически количество **worker_threads** должно соответствовать количеству потоков обработчиков почты CGPro, определенному в:

`Почта → Очередь → Установка в очередь → Обработчики`

Теоретическое количество писем в секунду, которое может обработать Kaspersky External-Helper, составляет `worker_threads+5`. Время, необходимое для проверки писем KAV/KAS, может уменьшить этот теоретический предел.

+5 относится к дополнительной работе, которую External-Helper может выполнить в течение секунды. Она ограничена 5 статическим сном в 0,2 секунды, чтобы сохранить использование процессора в ожидании, пока доступные рабочие потоки закончат свою работу.

Отладка внешнего помощника Kaspersky

Режим подробного журналирования CGPro

Для того чтобы внешний помощник мог вести полные журналы, необходимо активировать запись полных журналов в модуле сбора сообщений:

`Почта → Очередь → Установка в очередь → Уровень журнала : Всё`

Режим подробного журналирования помощника

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

```
DebugExternal = 1 // вывод вызовов файлов KAV/KAS в stdout/stderr

DebugFilterDaemon = 1 // слой абстракции движков и утилит KAV/KAS

DebugThreading = 1 // отчёты о работе потоков

DebugReporting = 0 // WebUI и консолидация данных

DebugConfig = 0 // отчёты о перезаписи файлов конфигурации KAV/KAS (пути в логах)
```

Инструмент диагностики

Инструмент диагностики позволяет вызывать самотестирование внешнего помощника Kaspersky вне CGPro. Он позволяет получить полный отчет, запустив движки KAV/KAS и отправив запрос на сканирование каждому из них.

Для получения лицензии диагностическому инструменту требуется запущенный CGPro. Инструмент диагностики не сможет запустить движки KAV/KAS, если внешний помощник Kaspersky уже запущен в CGPro.

Ниже приведен пример успешного тестирования инструментом диагностики со всеми отладочными флагами, установленными в 0:

```
# cd cgpro_home && ./Kaspersky/diagnose
# Проверка лицензии
* core/licensing.py License.set Kaspersky AntiSpam Accounts 25 loaded
* core/licensing.py License.set Kaspersky AntiVirus Accounts 25
loaded # Запуск и проверка демонов
* kaspersky/filterDaemon.py KasEngine.run Kaspersky Anti-Spam httpd service OK
* kaspersky/kassdk.py KAS_testScanner Kaspersky Anti-Spam file scanner OK
* kaspersky/kassdk.py KAS_httpd_kill Kaspersky Anti-Spam httpd service KO
* kaspersky/kavsdk.py KAV_license_init Kaspersky License OK
* kaspersky/kavsdk.py KAV_updater_init Kaspersky Threat database OK
```

```
* kaspersky/kavsdk.py KAV_httpd_run Kaspersky Anti-Virus httpd service OK
* kaspersky/kavsdk.py KAV_testScanner Kaspersky Anti-Virus file scanner OK
* kaspersky/kavsdk.py KAV_httpd_kill Kaspersky Anti-Virus httpd service KO
```