УТВЕРЖДЕН

BY.ИАДВ.00123-04 90 02-ЛУ

КОМПЛЕКС VBA32 ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Антивирусный фильтр для почтового сервера Postfix

Руководство администратора

BY.ИАДВ.00123-04 90 01

Листов 14

Подп. и дата	
Инв. N	
Взам. инв.	
Подп. и дата	
Инв.N	

2019

Литера

№ изм.	*Подп.*	*Дата*

АННОТАЦИЯ

Настоящий документ содержит руководство администратора антивирусного фильтра для почтового сервера Postfix, функционирующего под управлением ОС Linux (далее – Комплекс).

Разработчиком Комплекса является предприятие ОДО «ВирусБлокАда».

Комплекс предназначен для защиты клиентов почтовой системы от воздействия ВП и компьютерных вирусов, которые могут содержаться во входящих и исходящих почтовых сообщениях.

Комплекс обеспечивает:

- проверку всех почтовых сообщений на сервере перед доставкой получателю;
- гибкость и удобство настройки действий, выполняемых над почтовыми сообщениями, содержащими ВП или компьютерные вирусы, подозрительные файлы и неизвестные макросы: отсылка уведомлений, сохранение копий в заданном каталоге и отсылка по заданному почтовому адресу, добавление строк в тему письма и mime-заголовок;
- настройку политики безопасности по отношению к сообщениям ContentType=message/partial;
- использование файлов шаблонов для отсылаемых сообщений, настраиваемых администратором, а также возможность запуска заданной внешней программы при определенных событиях;
- использование эвристического анализатора антивирусного ядра увеличивает шансы обнаружения новых неизвестных вирусов и таким образом возможность предотвращения эпидемий новых вирусов;
- проверку множества архивов различных типов и файлов, упакованных различными упаковщиками;
- многопоточный режим работы фильтра и антивирусного демона;
- обновление антивирусных баз без перезагрузки.

Комплекс состоит из следующих модулей:

- vbapostfixf – модуль фильтра;
- vbapostfixf-pipe – модуль, обеспечивающий взаимодействие с Postfix
- vbaupdater – модуль обновления.

При работе программы используются ПК на базе архитектуры Intel x86.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Комплекс предназначен для защиты клиентов почтовой системы от воздействия вредоносных программ и компьютерных вирусов, которые могут содержаться во входящих и исходящих почтовых сообщениях.

Комплекс обеспечивает:

- проверку всех почтовых сообщений на сервере перед доставкой получателю;
- гибкость и удобство настройки действий, выполняемых над почтовыми сообщениями, содержащими вредоносные программы или компьютерные вирусы, подозрительные файлы и неизвестные макросы: отсылка уведомлений, сохранение копий в заданном каталоге и отсылка по заданному почтовому адресу, добавление строк в тему письма и mime-заголовок;
- настройку политики безопасности по отношению к сообщениям ContentType=message/partial;
- использование файлов шаблонов для отсылаемых сообщений, настраиваемых администратором, а также возможность запуска заданной внешней программы при определенных событиях;
- использование эвристического анализатора антивирусного ядра увеличивает шансы обнаружения новых неизвестных вирусов и таким образом возможность предотвращения эпидемий новых вирусов;
- проверку множества архивов различных типов и файлов, упакованных различными упаковщиками;
- многопоточный режим работы фильтра и антивирусного демона;
- обновление антивирусных баз без перезагрузки.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к техническим средствам

При работе программы используются ПК на базе архитектуры Intel x86. Аппаратная конфигурация ПК должна удовлетворять требованиям используемой ОС. Для установки Комплекса требуется не менее 500 МБ свободного дискового пространства на жестком диске ПК.

Минимальный объем ОЗУ – 500 МБ.

При использовании функции хранения копий инфицированных / подозрительных сообщений необходим достаточный объем свободного дискового пространства размер которого определяется потребностями пользователя.

2.2. Требования к программным средствам

Фильтр функционирует под управлением ОС Linux совместно с Postfix версии 2.1 и выше. В системе должна быть установлена библиотека glibc версии 2.18 и выше.

2.3. Общие характеристики входной и выходной информации

Входными данными для антивирусного фильтра являются почтовые сообщения в mime-формате, передаваемыми на проверку почтовой системой.

Выходными данными для антивирусного фильтра являются результаты проверки в виде числового (текстового) кода, сообщаемые фильтром почтовой системе.

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Установка

Антивирусный фильтр поставляется в виде архива vbapostfixf-[version].tar.gz, где version – версия пакета. Архив содержит:

- фильтр для Postfix;
- модуль обновления;
- конфигурационные файлы фильтра;
- скрипты установки / удаления, управляющий;
- описание применения.

Для установки фильтра выполнить следующие действия:

- распаковать архив: tar zxf vbapostfixf-[version].tar.gz;
- зайти в распакованную директорию: cd vbapostfixf-[version];
- запустить с правами суперпользователя скрипт установки: ./install;
- скопировать ключевой файл в /opt/vba/vba32.key;
- создать для фильтра пользователя vbauser и группу vbagroup;
- назначить параметры файлам фильтра:
  chown -R vbauser:vbagroup /etc/vba/vbapostfixf* /opt/vba/vbapostfixf
  /var/run/vba/vbapostfixf /var/log/vba /usr/bin/vbapostfixf-ctl
  chmod 0700 /usr/bin/vbapostfixf-ctl
  chmod 4700 /opt/vba/vbapostfixf/bin/vba*
- настроить взаимодействие фильтра и почтовой системы postfix. В конфигурационный файл Postfix «master.cf» добавить:
  filter unix - n n - 3 pipe
  flags=Rq user=vbauser argv=/opt/vba/vbapostfixf/bin/vbapostfixf-pipe -f ${sender} --
  ${recipient}
  smtp inet n - y - - smtpd -o content_filter=filter:dummy
- применить изменения: postfix reload

Установка Комплекса и интегрирование его с почтовой системой Postfix закончена.

3.2. Настройка

Конфигурационный файл vbapostfixf.conf разбит на секции, каждая из которых содержит логически связанные параметры. Для каждого параметра приводится краткое описание его назначения, затем могут быть приведены возможные значения, которые он может принимать.

Секция [Infected] содержит параметры, относящиеся к обработке инфицированных сообщений:

1) Action {cure, skip, discard} Определяет действие, выполняемое над инфицированными сообщениями.
   - cure – лечение сообщения;
   - skip – продолжить передачу сообщения пользователю;
   - discard – не доставлять сообщение пользователю.
2) CopyToDir {yes, no} Определяет возможность сохранения копии инфицированного сообщения.
   - yes – сохранять копию;
   - no – не сохранять копию.

3) CopyDirPath Путь к каталогу для сохранения копий инфицированных сообщений. Указать путь к существующему каталогу.
4) SenderNotify, RcptNotify {yes, no} Определяют возможность отсылки уведомлений отправителю (SenderNotify) и получателю (RcptNotify) инфицированного сообщения.
   - yes – отправлять уведомление;
   - no – не отправлять уведомление.
5) SenderNotifyTemplate, RcptNotifyTemplate Путь к шаблону отсылаемого уведомления.

Секция [Suspicious] содержит параметры, относящиеся к обработке подозрительных сообщений:

1) HeuristicLevel {0, 1, 2, 3} Определяет уровень эвристического анализатора:
   - 0 – отключен;
   - 1 – средний;
   - 2 – максимальный;
   - 3 – избыточный.

   Уровень эвристического анализатора определяет объем дополнительных действий, производимых антивирусным ядром при обработке объектов, для обнаружения новых неизвестных вредоносных программ и компьютерных вирусов. На почтовом сервере рекомендуется установить максимальный (2) уровень эвристического анализатора, для увеличения вероятности предотвращения эпидемий новых вирусов.
2) Action {skip, discard} Определяет действие, выполняемое над подозрительными сообщениями.
   - skip – продолжить передачу сообщения пользователю;
   - discard – не доставлять сообщение пользователю.

Назначение и возможные значения параметров CopyToDir, CopyDirPath, SenderNotify, RcptNotify, SenderNotifyTemplate, RcptNotifyTemplate аналогичны соответствующим в секции [Infected].

Секция [WithMacros] содержит параметры, относящиеся к обработке сообщений, содержащих неизвестные макросы. Назначение и возможные значения параметров Action, CopyToDir, SopyToDirPath, SenderNotify, RcptNotify, SenderNotifyTemplate, RcptNotifyTemplate аналогичны соответствующим в секции [Suspicious].

Секция [Notifications] описывает параметры настройки отсылки уведомлений администратору. Возможные значения параметров OnVirus, OnSuspicious, OnWithMacros, OnError, OnVirusTemplate, OnSuspiciousTemplate, OnWithMacrosTemplate, OnErrorTemplate аналогичны SenderNotify, SenderNotifyTemplate в секции Infected, далее приводится только общее описание их назначения:

1) OnVirus – отсылка уведомления об обнаруженном инфицированном сообщении;
2) OnSuspicious – отслылка уведомления об обнаруженном подозрительном сообщении;
3) OnWithMacros – отсылка уведомления об обнаруженном сообщении с неизвестными макросами;
4) OnError – отсылка уведомления о некоторой внутренней ошибке в Комплексе. Ошибкой является:
   - завершение срока действия ключевого файла (почтовый фильтр будет переведен в демонстрационный режим работы);
   - неправильно заданные значения параметров конфигурационного файла.

Секция [Syslog] содержит параметры записи в системный лог.

1) Level { None | Error | Warning | Info | Details | Debug } Уровень детализации
2) Facility { Daemon | Mail | Local0..7 } Способ записи в лог
3) Priority { Notice | Info | Debug } Уровень приоритета сообщений

Секция [Common] описывает параметры общего назначения:

1) Filter путь к бинарному файлу фильтра
2) Updater путь к бинарному файлу модуля обновления
3) KeyFile путь к ключевому файлу
4) RulesFile путь к файлу правил для определенных классов обнаруженных объектов
5) LockFile путь к файлу, где будет сохранен PID фильтра
6) PipeLog путь к лог-файлу vbapostfixf-pipe
7) FilterSocket путь к файлу-сокету, используемому фильтром
8) MailServer путь к бинарному файлу, обеспечивающему sendmail-интерфейс Postfix
9) BasesDir путь к каталогу с антивирусными базами
10) TmpDir путь к каталогу для временных файлов
11) BinDir путь к каталогу с бинарными файлами фильтра
12) TestDir путь к каталогу для хранения обновленных и ожидающих проверки администратором файлов
13) IniDir путь к каталогу, где хранить файл, описывающий обновление
14) UpdateTmpDir путь к каталогу для временных файлов при обновлении
15) UpdateType { UPDATE_ALL | UPDATE_BASES | DOWNLOAD_ONLY } тип обновления
16) UpdateFrom путь к ресурсу обновления
17) ProxyAddress адрес прокси-сервера
18) ProxyUser пользователь прокси-сервера
19) EnableNtlm { on | off } использовать ли NTLM-аутентификацию при обновлении
20) PassiveFtp { on | off }использовать ли пассивный режим при обновлении с ftp-ресурса
21) LogDir путь к каталогу для лог-файлов
22) LogFile { yes | no } указывает, будет ли фильтр писать лог-файлы
23) UpdaterLog { yes | no } указывает, будет ли модуль обновления писать лог-файлы
24) MaxLogNum { положительное число } указывает количество хранящихся последних лог файлов
25) MaxLogSize { > 10000 } указывает максимальный размер лог файла в байтах.
26) Threads максимальное число потоков, одновременно проверяющих сообщения
27) FilterMail Определяет почтовый адрес, указываемый в поле `From:` каждого сообщения, отправленного почтовым фильтром (например, уведомления пользователю, администратору).
28) AdminMail Определяет почтовый адрес администратора почтовой системы, по которому будут при необходимости отправляться служебные сообщения/уведомления.
29) MarkMessage {yes, no} Определяет возможность добавления в RFC-822 заголовок сообщения строки о результате проверки сообщения.
    - yes – добавлять строку в заголовок сообщения;
    - no – не добавлять строку в заголовок сообщения.
30) MarkSubject {yes, no} Определяет возможность добавления в тему сообщения строки вида [VBA32: result], где result отражает результат проверки сообщения.
    - yes – добавлять строку в тему сообщения;
    - no – не добавлять строку в тему сообщения.
31) MessagePartialDiscard {yes | no} Определяет действие почтового фильтра при обработке сообщений, имеющих поле `Content-Type = message/partial`.
    - yes – отбрасывать сообщения, не проверяя; при этом сообщение не доставляется пользователю;
    - no – продолжить проверку сообщения.

32) NotifySenderPartial, NotifyRcptPartial {yes | no} Определяют возможность отсылки уведомлений отправителю (SenderNotify) и получателю (RcptNotify) сообщения с полем `Content-Type = message/partial`.
   - yes – отправлять уведомление;
   - no – не отправлять уведомление.

33) SenderPartialTemplate, RcptPartialTemplate Пути к шаблонам уведомлений пользователей о сообщении с полем Content-Type=message/partial. Значения параметров аналогичны вышеописанным SenderNotifyTemplate и RcptNotifyTemplate.

Могут быть приняты следующие сценарии работы с сообщениями Content-Type=message/partial. Если MessagePartialDiscard = yes, то сообщение отбрасывается почтовым сервером и не доставляется пользователю. При этом если NotifySenderPartial = yes, то отправитель письма получит уведомление, указанное параметром SenderPartialTemplate. При NotifyRcptPartial = yes получатель получает уведомление. Если MessagePartialDiscard = no, сообщение пропускается почтовым сервером (если при проверке оно оказалось «чистым»). При этом остаются справедливыми правила отсылки уведомления, описанные выше. То есть в этом случае есть возможность уведомить получателя письма о потенциальной опасности данного сообщения из-за невозможности его целостной проверки на почтовом сервере.

При необходимости можно модифицировать или создавать новые файлы шаблонов уведомлений. В начале файла шаблона можно добавить несколько полей для MIME заголовка (Subject, Content-Type, MIME-Version). Сообщение может содержать подставляемые фильтром параметры:
%SENDER% - заменяется фильтром на почтовый адрес отправителя сообщения;
%RCPT% - заменяется фильтром на почтовый адрес получателя сообщения;
%SUBJECT% - заменяется фильтром на тему сообщения;
%VIRUS_LIST% - заменяется фильтром на список вредоносных объектов, найденных в сообщении.

3.3. Применение изменений

После изменения конфигурации фильтра выполнить vbapostfixf-ctl reload.

3.4. Обновление

Для обновления выполнить vbapostfixf-ctl update.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными для фильтра являются почтовые сообщения в mime-формате, передаваемые на проверку почтовой системой.

Выходными данными являются результаты проверки в виде числового (текстового) кода, сообщаемые фильтром почтовой системе.

5. ОСНОВНЫЕ МЕРЫ ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

5.1. Организационные меры защиты

Основными организационными мерами обеспечения защиты от воздействия ВП, позволяющими уменьшить риск заражения ресурсов вычислительной техники и минимизировать отрицательные последствия в случае попадания ВП в вычислительную систему, являются следующие:

1) обучение пользователей правилам безопасности, путям и причинам распространения ВП, методам профилактики;
2) разработка инструкций и правил работы, контроль их выполнения;
3) разработка плана действий пользователей и должностных лиц по локализации возможных ВП для уменьшения ущерба;
4) разработка и внедрение правил, исключающих возможности использования не проверенного (не лицензионного) ПО.

5.2. Организационно-технические меры защиты

Правильная настройка ПО, установление минимально необходимых прав доступа пользователей к ресурсам вычислительной техники позволяют уменьшить риск заражения и потери. Следующие организационно – технические меры позволяют уменьшить потенциальную опасность от атак компьютерных вирусов:

1) отключение в BIOS SETUP загрузки с дискеты;
2) использование режима «защита загрузочного сектора от записи» в BIOS;
3) резервное копирование ценной информации;
4) установление минимально необходимых прав доступа к сетевым ресурсам.

5.3. Профилактика

Систематическая проверка целостности ПО с помощью программ защиты от воздействия ВП позволяет предупредить массовое распространение ВП. Одной из обязательных мер профилактики является проверка всей входящей информации.

В критических местах технологических звеньев серьезной профилактической мерой будет использование форматов документов, не содержащих управляющих структур (например «.TXT», «.RTF»).

6. МАРКИРОВКА СЕРТИФИЦИРУЕМОЙ ПРОДУКЦИИ

Знак соответствия, приведенный на рис. 1, означает, что Комплекс соответствует требованиям ТР 2013/027/BY.

Рис. 1

Знак соответствия, приведенный на рис. 2, означает, что система менеджмента качества применительно к проектированию, производству и технической поддержке Комплекса соответствует требованиям СТБ ISO 9001.

Рис. 2

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе использованы следующие сокращения:
ВП – вредоносная программа;
ИТ – информационная технология;
ОС – операционная система;
ПК – персональный компьютер.

Лист регистрации изменений									
Номера листов (страниц)					*Всего листов (страниц) в докум.*	*№ документа*	*Входящий № сопроводи-тельного докум. и дата*	*Подп.*	*Дата*
Изм.	*изменен-ных*	*заменен-ных*	*новых*	*аннули-рованных*					

№ изм.	*Подп.*	*Дата*