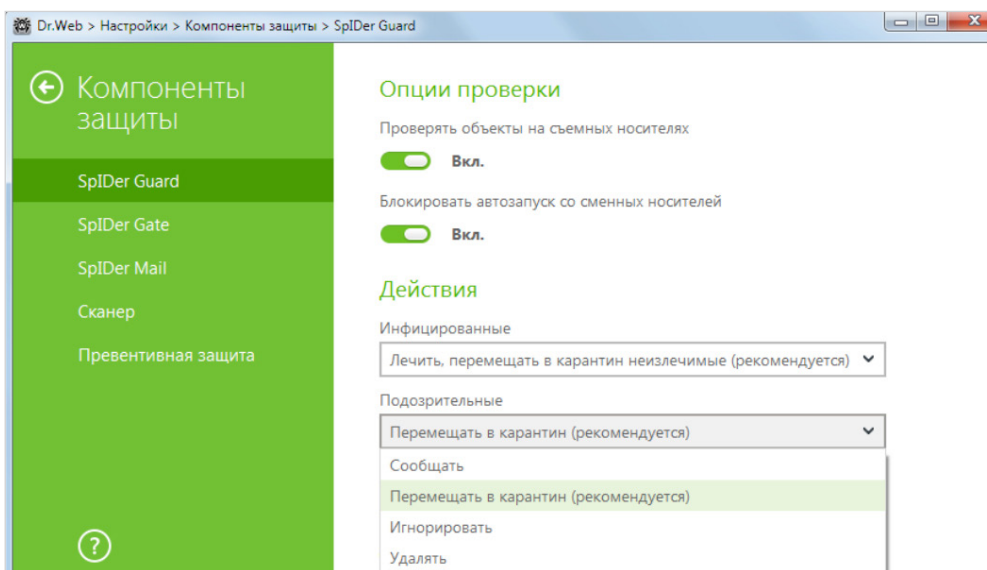


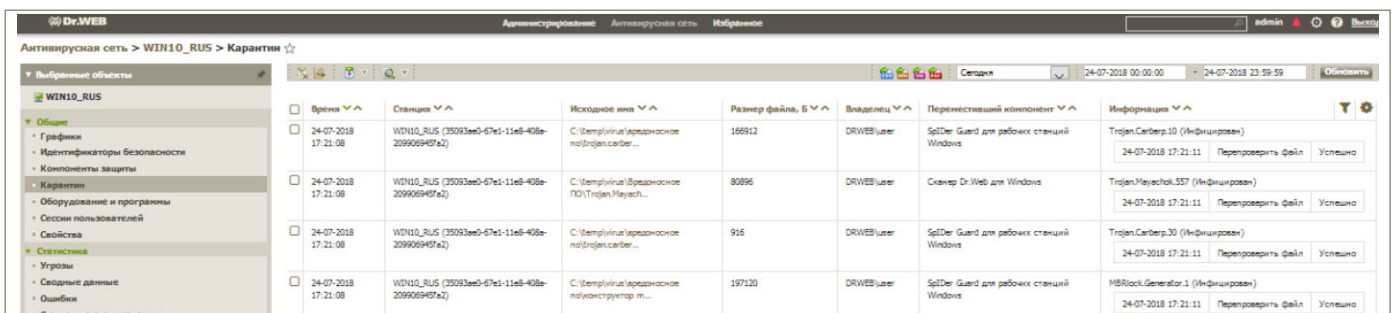


Использование Dr.Web vxCube в работе системного администратора

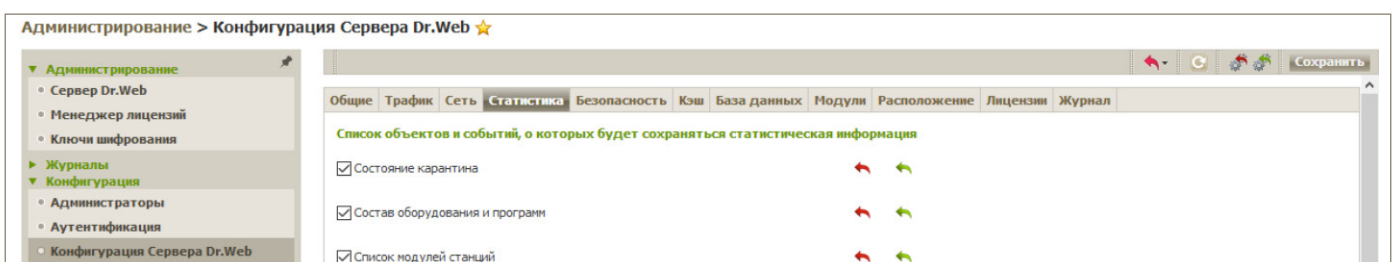
В работе системного администратора встречаются не только вирусы и троянцы. Иногда невозможно с первого раза определить, является найденный файл вредоносным или нет. Антивирус таким файлам присваивает статус Подозрительный. Настройка по умолчанию для таких файлов — перемещать в карантин. Проверить это можно в настройках локального Агента Dr.Web или в Центре управления Dr.Web.



Для того чтобы проанализировать вызывающий подозрение файл, откройте Центр управления Dr.Web, перейдите в раздел карантина (**Администрирование** → **Карантин**). С помощью фильтра выберите нужный промежуток времени и найдите интересующий файл.

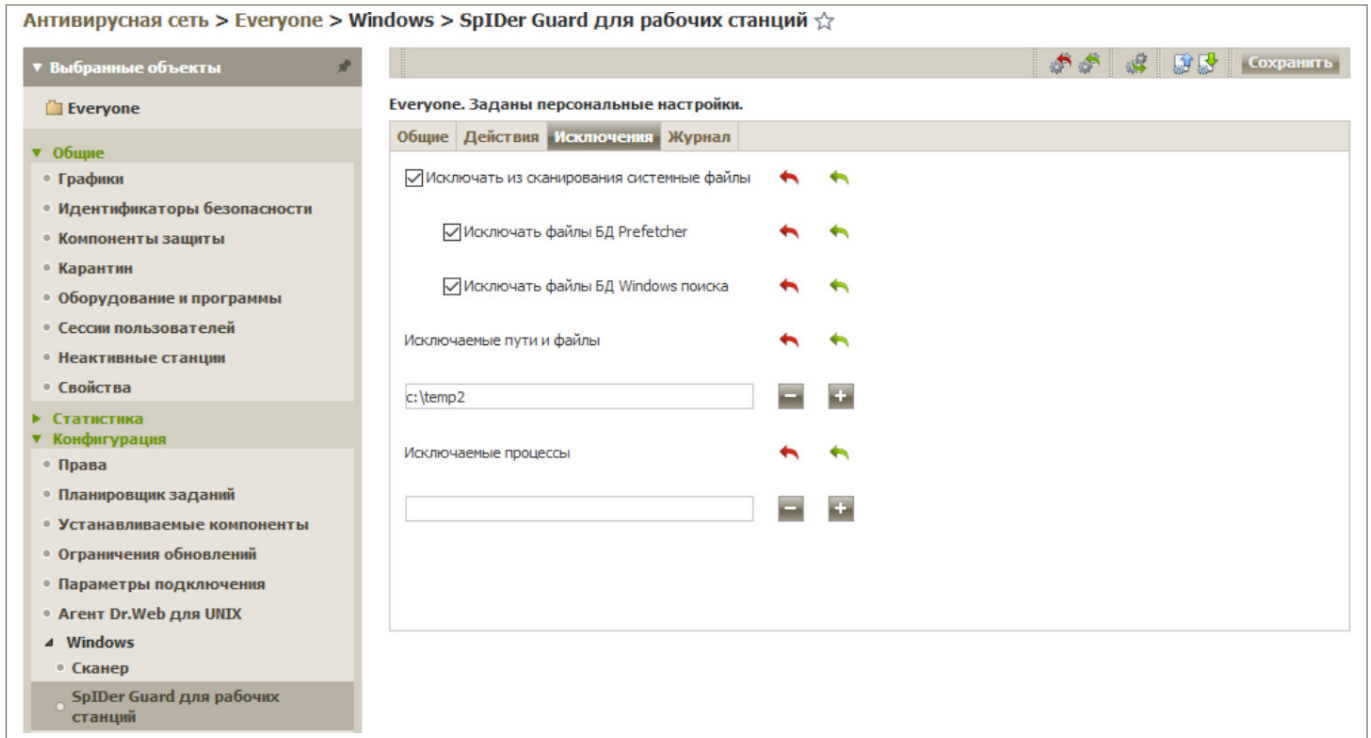


! Если в меню Антивирусная сеть Центра управления отсутствует пункт Карантин, перейдите в раздел **Администрирование** → **Конфигурация Сервера Dr.Web** и на закладке **Статистика** отметьте пункт **Состояние карантина**.



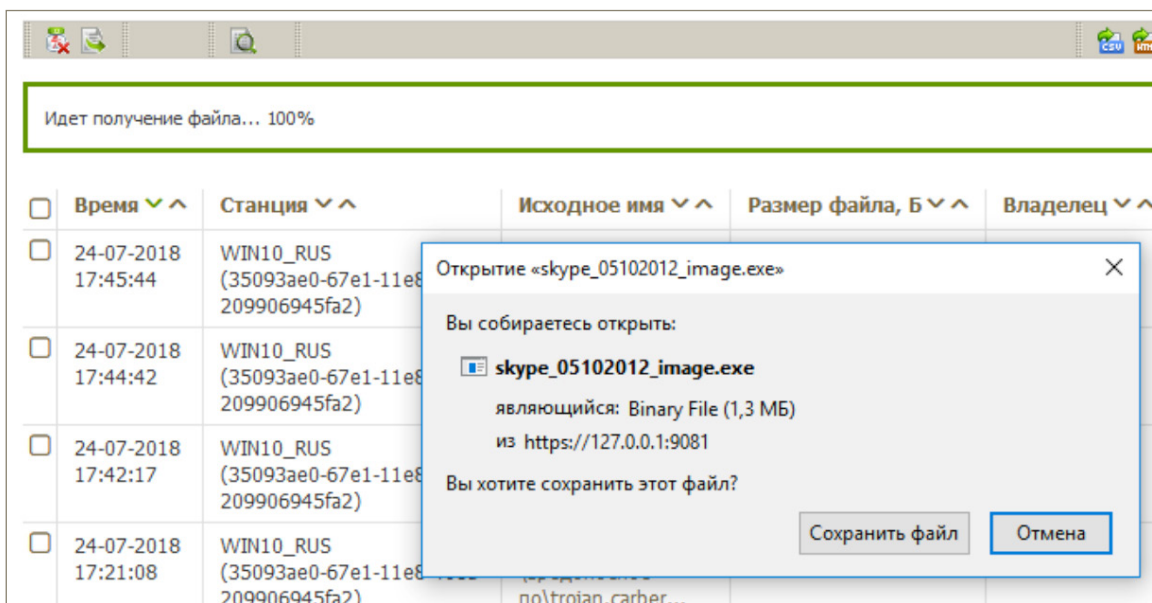
Файл из карантина для анализа нужно загрузить на рабочую станцию. Поскольку файл вредоносный (хотя и со статусом Подозрительный), то антивирус на рабочей станции, естественно, не должен дать сохранить такой файл. Первая идея — отключить антивирус. Этого делать нельзя. Выберите станцию, на которую будет сохранен файл, в **Антивирусной сети** и в разделе **SpIDer Guard** перейдите на закладку **Исключения**. Добавьте директорию, куда будет сохранен файл для анализа.

! Не рекомендуется в качестве такой директории назначать директорию, куда по умолчанию сохраняются файлы, лучше создать специальную.

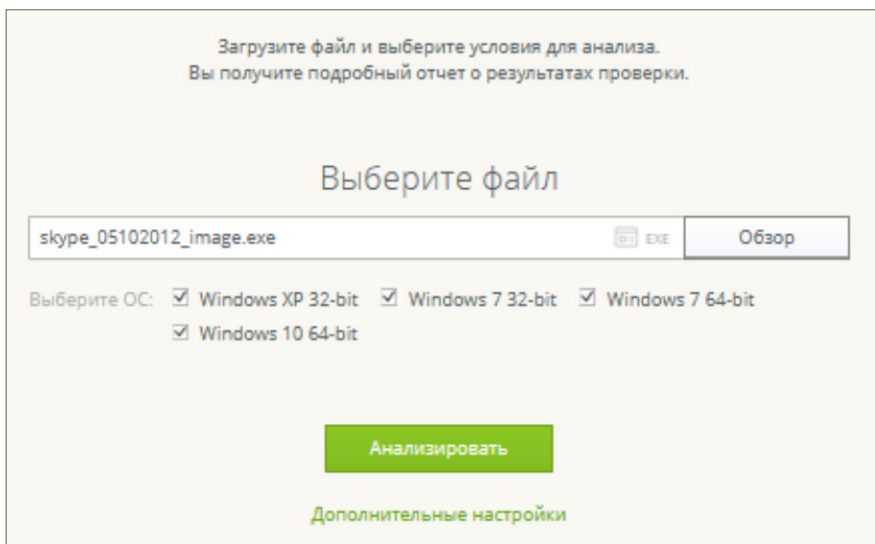


Настроив **Исключения**, вернитесь в раздел **Карантин**, выберите нужный файл, отметьте его, нажмите на иконку **Экспорт** и сохраните файл в нужную директорию.

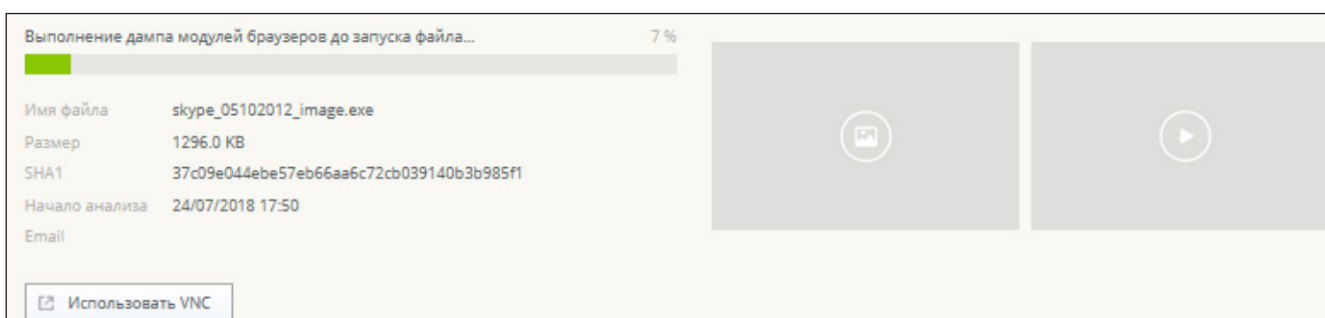
<input type="checkbox"/>	24-07-2018 17:21:08	WIN10_RUS (35093ae0-67e1-11e8-408a-209906945fa2)	C:\temp\virus\вредоносное по\конструктор м...	197120	DRWEB\user	SpIDer Guard для рабочих станций Windows	MBRlock.Generator.1 (Инфицирован)	24-07-2018 17:21:11	Перепроверить файл	Успе...
--------------------------	---------------------	--	---	--------	------------	--	-----------------------------------	---------------------	--------------------	---------



Откройте окно сервиса vxCube, загрузите сохраненный файл и выберите тестовое окружение.



Дождитесь момента окончания проверки.

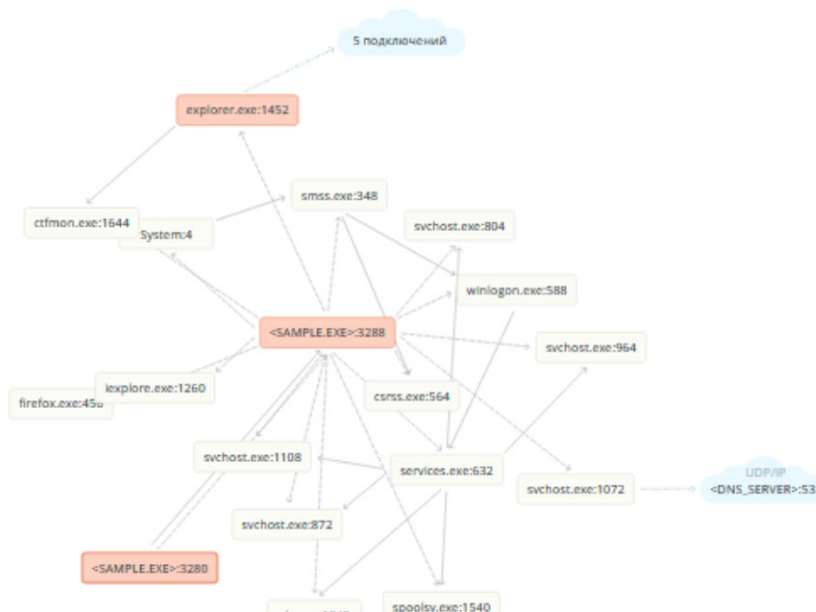


По окончании проверки в некоторых случаях можно просмотреть видео с записью действий вредоносного файла. Прокрутите отчет и изучите описание поведения проверенного файла.

Поведение

Вредоносное	Несанкционированное внедрение в системный процесс, Несанкционированное внедрение в процесс браузера, Удаление оригинального файла
Подозрительное	Обеспечение автозагрузки с помощью стандартной ветви реестра Software\Microsoft\Windows\CurrentVersion\Run
Нейтральное	Несанкционированное внедрение в новый процесс, Создание файла в каталоге %AppData%, Создание окна, DNS-запрос, Попытка подключения, Отправка HTTP-запроса методом GET, Установка перехватов функций в браузере

В нашем примере анализ показал, что поведение файла однозначно вредоносное. Поэтому изучите, какие файлы, процессы, ресурсы вызывает анализируемый (уже точно) вредоносный файл.



Для обеспечения автозапуска и распространения:

Модифицирует следующие ключи реестра:

```
[<HKCU>\Software\Microsoft\Windows\CurrentVersion\Run] 'Qhjvj' = '%APPDATA%\Qhjvj.exe'
```

Вредоносные функции:

Внедряет код в следующие системные процессы:

```
<SYSTEM32>\alg.exe
```

следующие пользовательские процессы:

```
firefox.exe
```

Перехватывает функции в браузерах

```
Процесс firefox.exe, модуль dnsapi.dll
```

```
Процесс firefox.exe, модуль ws2_32.dll
```

```
Процесс iexplorer.exe, модуль ws2_32.dll
```

```
Процесс iexplorer.exe, модуль wininet.dll
```

Изменения в файловой системе:

Создает следующие файлы:

```
%APPDATA%\qhjvj.exe
```

Самоудаляется.

Сетевая активность:

Подключается к:


```
'api.wipmania.com':80
```

Сервис vxCube отдельно перечисляет создаваемые файлы. Типичным приемом, применяемым злоумышленниками, является перешифрование вредоносного файла в надежде, что его новый вариант не будет распознан антивирусом. А вот файлы внутри перешифрованного контейнера, скорее всего, не изменятся. И если вы вдобавок к антивирусу используете нечто типа CERT — вы можете добавить их как признак компрометации.

И в заключение список сетевых ресурсов, к которым обращался вредоносный файл. Скорее всего, это командные центры, и не вредно будет добавить их в черный список запрещенных ресурсов.

Созданные файлы [1] <u>Файлы и дампы памяти</u> [14]		
Путь	SHA1	Обнаружено
%APPDATA%\qhjvj.exe	37c09e044ebe57eb66aa6c72cb039140b3b985f1	BackDoor.IRC.NgrBot.146

1-1 из 1 | 10



Протокол	Адрес	Данные прикладного уровня
IP	cantvenlinea.biz:1863	—
TCP/IP	api.wipmania.com:80	HTTP GET http://api.wipmania.com/
UDP/IP	<DNS_SERVER>:53	DNS ASK pluto.iziger.pl
UDP/IP	<DNS_SERVER>:53	DNS ASK cantvenlinea.biz
UDP/IP	<DNS_SERVER>:53	DNS ASK photobeat.su

Используя раздел **Офисный контроль**, добавьте выявленные вредоносные ресурсы в черный список.

! Запретить доступ к вредоносным ресурсам можно сразу для всех станций, выбрав группу **Everyone**.

Антивирусная сеть > Everyone > Windows > Офисный контроль ☆

Выбранные объекты

- Everyone
- Общие
- Статистика
- Конфигурация
 - Права
 - Планировщик заданий
 - Устанавливаемые компоненты
 - Ограничения обновлений
 - Параметры подключения
 - Агент Dr.Web для UNIX
 - Windows
 - Сканер
 - SrIDer Guard для рабочих станций
 - Офисный контроль

Общие Пользовательские

Everyone. Заданы персональные настройки.

Пользователи

- Администраторы
- Гости
- Пользователи

Общие Белый список Сохранить

Используйте черный и белый списки, чтобы указать веб-сайты, доступ к которым должен быть разрешен или, наоборот, запрещен.

Белый список

←
→

Черный список

←
→

Каталоги и файлы



ООО «Доктор Веб»,
2003 — 2018

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Телефон (многоканальный): +7 495 789-45-87 | Факс: +7 495 789-45-97
<https://антивирус.рф> | <https://www.drweb.ru> | <https://curenet.drweb.ru/> | <https://free.drweb.ru/>

