

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.

🔯 Dr.Web > Настройки > Компоненты защиты >	SpIDer Guard				
Компоненты защиты	Опции проверки Проверять объекты на съемных носителях				
SpIDer Guard					
SpIDer Gate	Вкл.				
SpIDer Mail	Лейстрия				
Сканер	Инфицированные				
Превентивная защита	Лечить, перемещать в карантин неизлечимые (рекомендуется) 💙				
	Подозрительные				
	Перемещать в карантин (рекомендуется)				
	Сообщать				
	Перемещать в карантин (рекомендуется)				
0	Игнорировать				
	Удалять				

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.

₩Dr.WEB			Аднинистри	рование Антивирусная сёть	Избранное				admin 🐥	O 🛛 🔤
Антивирусная сеть > WIN10_RUS > Ка	рантин 🏠									
Выбранные объекты	*	🥻 🎽 🕈 🔻	Q v			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	🔓 🏪 Сегодня 🔍 24	+07-2018 00:00:00 - 2	4-07-2018 23:59:59	Обновить
WIN10_RUS		Вреня УА	Станция	Искодное иня УА	Разнер файла, Б У А	Владелец	Перенестивший конпонент У А	Информация У А		TC
* Ofcapre	0	24-07-2018	WIN10_RUS (35093se0-67e1-11e8-408s-	C:\temp\virus\speapHocHoe	166912	DRWEB\user	SpIDer Guard для рабочих станций	Trojan.Carberp.10 (Инфи	цирован)	
 Идентификаторы безопасности 		17:21:08	209906945fa2)	no\trojan.carber			Windows	24-07-2018 17:21:11	Перепроверить файл	Успешно
• Компоненты защиты Карантин	0	24-07-2018	WIN10_RUS (35093se0-67e1-11e8-408s-	C:\temp\virus\Вредоносное	80896	DRWEB\user	Сканер Dr.Web для Windows	Trojan,Mayachok,557 (Ино	фицирован)	
• Оборудование и программы		17:21:08	209906945fa2)	ND\Trojan.Mayach				24-07-2018 17:21:11	Перепроверить файл	Успешно
 Сессии пользователей Свойства 	0	24-07-2018	WIN10_RUS (35093ae0-67e1-11e8-408a-	C:\temp\virus\spegpнocнoe	916	DRWEB\user	SpIDer Guard для рабочих станций	Trojan Carberp 30 (Vi+qui	цирован)	
Статистика		17:21:08	209906945fa2)	no\trojan.carber			Windows	24-07-2018 17:21:11	Перепроверить файл	Успешно
 Угрозы Сводные данные 	0	24-07-2018	WIN10_RUS (35093ae0-67e1-11e8-408a-	C:\temp\virus\вредоносное	197120	DRWEB\user	SpIDer Guard для рабочих станций	MBRJock.Generator.1 (Ин	фицирован)	
• Ошибки		17:21:08	209906945fa2)	па\канструктар т			Windows	24-07-2018 17:21:11	Перепроверить файл	Успешно

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.

Администрирование > Конфигура	ция Сервера Dr.Web 🖕		
▼ Администрирование		h- С 💣 🖉 Сохрани	ть
 Сервер Dr.Web Менеджер лицензий Ключи шифрования 	Общие Трафик Сеть Статистика Безопасность Кэш База данных Список объектов и событий, о которых будет сохраняться статистическ	Модули Расположение Лицензии Журнал ская информация	î
► Журналы ▼ Конфигурация	Состояние карантина	• •	
АдминистраторыАутентификация	Состав оборудования и програми	* *	
 Конфигурация Сервера Dr.Web 	Список модулей станций	* *	

Dr.WEB® Enterprise Security Suite

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.

Антивирусная сеть > Everyone > Wi	ndows > SpIDer Guard для рабочих ста	ций			
▼ Выбранные объекты 🕺				🦸 🦨 🥵 💱 🛃 Сохранить	
🗀 Everyone	Everyone. Заданы персональные настройки.				
▼ Общие	Общие Действия Исключения Журнал				
• Графики	Исключать из сканирования системные файлы	+	•		
 Идентификаторы безопасности Компоненты защиты 	🗹 Исключать файлы БД Prefetcher	•	•		
 Карантин Оборудование и программы 	🗹 Исключать файлы БД Windows поиска	•	*		
 Сессии пользователей Неактивные станции 	Исключаемые пути и файлы	•	•		
• Свойства	c:\temp2		+		
СтатистикаКонфигурация		-	-		
• Права	naono acciole ripodecen				
 Планировщик заданий Устанавливаемые компоненты 		-	+		
• Ограничения обновлений					
• Параметры подключения					
• Агент Dr.Web для UNIX					
▲ Windows					
• Сканер					
SpIDer Guard для рабочих станций					

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

	24-07-2018	WIN10_RUS	C:\temp\virus	197120 DRWEB\user SpIDer Guard для рабочих ста		SpIDer Guard для рабочих станций	MBRlock.Generator.1 (Инф	фицирован)	
	17:21:08	(35093ae0-6/e1-11e8-408a- 209906945fa2)	\вредоносное по\конструктор m			windows	24-07-2018 17:21:11	Перепроверить файл	Ус
	💑 🛃	Q					6		
	Идет полу	чение файла 100%	~^	Исходное и		Размер файла БУА	Влалелец У А		
		eranqua		пекодност		тазнер фанла, в	ынделец		
	J 24-07- 17:45:	-2018 WIN10_RU :44 (35093ae0 20990694	IS)-67e1-11e8 Отк 5fa2)	рытие «skype_0510	2012_image.e	exe»	×		
	7 24 07	2010	Вы	собираетесь откр	ыть:		-		
	17:44:	:42 (35093ae0 20990694)-67e1-11e8 [5fa2)	skype_0510201 являющийся: В	2_image.exe Sinary File (1,3	а 3 МБ)			
C	24-07-	-2018 WIN10_RU :17 (35093ae0	IS)-67е1-11е8 _{Вы}	из https://127.0.	.0.1:9081 этот файл?				
		20990694	5fa2)						
C	24-07-	-2018 WIN10_RU :08 (35093ae0	IS)-67e1-11e8		har	Сохранить файл	Отмена		
	1	20990094	51021	IIU\UIUIdil.Cdl	Del				

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

	Вы получите подробный отчет о	результатах проверки.	
	Выберите	файл	
skype_051020	12_image.exe	EXE	Обзор
ыберите ОС:	 ✓ Windows XP 32-bit ✓ Windows ✓ Windows 10 64-bit 	s 7 32-bit ⊻ Windows 7	64-bit
	Анализирова	ать	

Дождитесь момента окончания проверки.

Выполнение дамг	та модулей браузеров до запуска файла	7 %				
Имя файла Размер SHA1 Начало анализа	skype_05102012_image.exe 1296.0 KB 37c09e044ebe57eb66aa6c72cb039140b3b985f1 24/07/2018 17:50					
Етаіl						

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 оригинальног файла
Подозрительное	Обеспечение автозагрузки с помощью стандартной ветви peecrpa 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.

- +



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 невредно будет добавить их в черный список запрещенных ресурсов.

Созданные файлы [1]	Файлы и дампы памяти [14]	
Путь	▲ SHA1	Обнаружено
%APPDATA%\qhjvjl.exe	37c09e044ebe57eb66aa6c72cb039140b3b985f1	BackDoor.IRC.NgrBot.146
		1-1 из 1 10 .



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 > Wi	ndows > Офисный контроль 🚖	
▼ Выбранные объекты 🕺	Общие Пользовательские	4 D 🕹
🗀 Everyone	Everyone. Заданы персональные настройки.	
 Общие Статистика Конфигурация Права Планировщик заданий Устанавливаемые компоненты Ограничения обновлений 	 Пользователи Администраторы Гости Пользователи 	Общие Белый список Сохранить используите черным и оелым списки, чтооы указать вео-саиты, доступ к которым должен быть разрешен или, наоборот, запрещен. Белый список
 Параметры подключения Агент Dr.Web для UNIX Windows Сканер SpIDer Guard для рабочих станций 		Черный список 🔄 🥎
 Офисный контроль 		Каталоги и файлы



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.pф | https://www.drweb.ru | https://curenet.drweb.ru/ | https://free.drweb.ru/

