

## How Dr.Web vxCube can assist system administrators in their work





## How Dr.Web vxCube can assist system administrators in their work

As they go about their work, system administrators encounter more than Trojans and viruses. Sometimes it's hard for them to tell at first glance whether a file is actually malicious. The antivirus may flag it as suspicious. As a rule, files of this kind are moved by default to the quarantine. You can check the corresponding option in the Agent's settings or in the Dr.Web Control Center.



To analyse a suspicious file, open the Dr.Web Control Center and go to the quarantine section (**Administration**  $\rightarrow$  **Quarantine**). Use the filter to specify the desired period of time and to find the file you need to examine.

Anti-virus Network > WIN10_RUS > Quarantine 🏠												
▼ Selected objects	ŝ	🗴 🗟 🛛 🖥 🔻	Q v		😤 🚔 🛍 i	Today	✓ 06-08-2018 00:0	0:00 - 06-	08-2018 23:5	9:59	Refre	sh
WIN10_RUS	_	Time M.A	Chaling M.A.	Original second of a	Tile size Dat a	0	Manual has a second set of	Televention				~
	U	Time * A	Station	Original name * A	rile size, b * A	Owner * A	Proved by component * A	Information	~~			
▼ General		06-08-2018	WIN10 RUS	C:\temp\virus	166912	DRWEB\user	SpIDer Guard for Windows	Trojan.Carberp	. 10 (Infecte	ed)		
Charts		13:42:12 (6d7c1) 1c97aft	(6d7c12e0-9963-11e8-725c- 1c97af6cd506)	\вредоносное no\trojan.carber			workstations					
<ul> <li>Security identifiers</li> </ul>								06-08-2018	Rescan	Success		
• Protection components								13:42:16	file			
Quarantine	O	06-08-2018	WIN10 RUS	C:\users	197120	DRWEB\user	SpIDer Guard for Windows	MBRlock.Genera	ator. 1 (Infe	cted)		
• Hardware and software		13:42:11	(6d7c12e0-9963-11e8-725c-	\user\appdata\local			workstations					
• Users sessions			1c97af6cd506)	\temp\rwz2ds1t				06-08-2018	Rescan	Success		
• Properties								13:42:16	nie			
<ul> <li>Statistics</li> </ul>		06-08-2018	WIN10_RUS	C:\temp\virus	80896	DRWEB\user	Dr.Web Scanner for Windows	Trojan.Mayach	ok. 557 (Infe	ected)		
<ul> <li>Configuration</li> </ul>		13:42:11	(6d7c12e0-9963-11e8-725c-	Вредоносное								
Permissions			1c97af6cd506)	∏O\Trojan.Mayach			06-08-2018	Rescan	Success	SS		
• Task Scheduler								13:42:15	file			



If the Quarantine item is not available in the Anti-virus network menu, go to Administration  $\rightarrow$  Dr.Web Server Configuration. In the Statistics tab, tick the box Quarantine state.

Administration > D	r.Web Server confi	guration 🏠		
<ul> <li>Administration</li> <li>Logs</li> <li>Configuration</li> </ul>	*	Ganaval Traffic Natural Statistics Security Cache	Database Medular Location Licenses Loc	🔨 - 🖸 🏕 Save
Administrators     Authentication		The list of objects and events about which statistic inform	ation will be stored	
Dr.Web Server conf	guration	Quarantine state	♠ ♠	
Or.Web Server remo     Or.Web Server Task	te access Scheduler	Hardware and software composition	<b>•</b> •	
Web Server configure     User hooks	ation	☑ List of the station modules	<b>•</b> •	

To examine a quarantined file, you must download it to a computer. Because the file is suspicious, the anti-virus protecting the PC will prevent the file from being saved on the hard drive. Disabling the anti-virus is a bad idea. Instead, select the host on which the file is to be saved. In **Anti-virus network**, select the **SpIDer Guard for workstations** section, and open the **Exclusions**. tab. Add the directory in which you want to store the suspicious file for analysis.

! It is not recommended to add your download folder to the exclusions list. Instead, create a separate directory.

Anti-virus Network > WIN10_RUS > V	Windows > SpIDer Guard for workstations $ m cm$		
▼ Selected objects			🦸 🖑 🦂 🖉 🖉 🛃 Save
WIN10_RUS	WIN10_RUS. Custom settings are specified.		
<ul> <li>General</li> <li>Statistics</li> <li>Configuration</li> </ul>	General         Actions         Exclusions         Log           Exclude system files from the scan	<b>*</b> *	
Permissions     Task Scheduler	Exclude Prefetcher DB files	• •	
• Installing components • Update restrictions	Exclude Windows search DB files	<b>*</b> *	
Connection settings     Scanner	Excluded paths and files	• •	
<ul> <li>SpIDer Mail and SpIDer Gate</li> <li>Dr.Web Agent</li> </ul>	c:\temp2		
<ul> <li>Preventive protection</li> <li>Dr.Web Firewall</li> </ul>	Excluded processes	* *	
Or.Web for Microsoft Exchange Server     Network port monitor		- +	
SpIDer Guard for workstations			

Once the folder is added to **Exclusions**, return to the **Quarantine** section. Select the file, click **Export**, and save the file to the appropriate directory.

	06-08-2018	WIN10_RUS	C:\temp\virus	197120	DRWEB\	user SpIDer Guard fo	or Window	s MBRI	ock.Genera	ator. 1 (Infe	cted)	
	13,72,11	(00701220-3505-1128-7250- 1c97af6cd506)	по\конструктор m			WORKSLAUOUS		06- 13:	08-2018 42:15	Rescan file	Succes	s
į	🖍 🗟 🛛 🕏 🔻	Q V		<b>*</b> * * *	Today	✓ 06-0	8-2018 00:0	D:00 - C	5-08-2018 2	3:59:59	Refr	esh
	Time 🔨 🔨	Station Y ^	Original name 🗸 🔨	File size, B Y ^	Owner Y ^	Moved by compone	ent V ^	Informatio	×^		T	•
	06-08-2018 13:42:12	WIN10_RUS (6d7c12e0-9963-11e8-725c- 1c97af6cd506)	C:\temp\virus Открытие «skype_0510. Вы собираетесь откр	166912 2012_image.exe» ыть:	DRWEB\user	SoIDer Guard for Wind X	lows	Trojan.Carbe 06-08-2018 13:42:16	rp. 10 (Infe Rescar file	cted) Success		
	06-08-2018 13:42:11	WIN10_RUS (6d7c12e0-9963-11e8-725c- 1c97af6cd506)	skype_0510201. являющийся: В из https://127.0.	2_image.exe inary File (1,3 MB) 0.1:9081			WS	MBRlock.Gen 06-08-2018 13:42:16	erator. 1 (Ir Rescar file	fected) Success		
	06-08-2018 13:42:11	WIN10_RUS (6d7c12e0-9963-11e8-725c- 1c97af6cd506)	Вы хотите сохранить	этот файл?	Сохранить фа	ийл Отмена	dows	Trojan.Mayao 06-08-2018 13:42:15	hok. 557 (I Rescar file	nfected) I Success		
	06-08-2018 13:42:11	WIN10_RUS (6d7c12e0-9963-11e8-725c- 1c97af6cd506)	C:\users \user\appdata\local \temp\qv7kkox2	197120	DRWEB\user	SpIDer Guard for Wind workstations	lows	MBRlock.Gen 06-08-2018 13:42:15	Rescar	fected) Success		

Open the vxCube window, upload the saved file, and set up your test environment.



Upload a file and configure environment for analysis. The file will be thoroughly analysed, and results will be reported shortly.						
		Choose file				
Trojan.Carb	erp.647.exe		EXE	Browse		
Choose OS:	☑ Windows XP 32-bit □ Windows 10 64-bit	U Windows 7 32-bit	□ Windows 7 6	i4-bit		
		Analyze				
		Additional settings				

## Wait while the file is being analysed.

Dumping browser	7.5		
Filename	Trojan.Carberp.647.exe		
5ize	335.5 KB		
SHA1	c1c6d7fa967d4e95d8b61	ae8c21a66c3f87cae28	
Analysis started	17/07/2018 16:42		
Email	la@downh.com		
🖾 Use VNC			

In some cases, when the analysis is complete, you can watch a video showing what the malicious file has been doing in the system.

Look through the report and read the description of the file's behaviour.

Behavior	
Malicious	Unauthorized injection to a system process, Enabling autorun with Startup directory, Deleting of the original file, Forced shutdown of a browser
Suspicious	No data
Neutral	Creating a window, Unauthorized injection to a recently created process, Creating a file in the %temp% directory, Deleting a recently created file, Enabling the 'hidden' option for recently created files, Launching a process, DNS request, Searching for the window, Searching for the browser window. Connection attempt

In our example, the analysis showed that the file was definitely malicious. Then check what files, processes, and components were used by the analysed malicious (now that we've established that for sure) file.





Malicious functions:	Injects code into the following system processes: <system32>\svchost.exe Terminates or attempts to terminate</system32>
	the following user processes: iexplore.exe firefox.exe
Modifies file system:	Creates the following files: %TEMP%\1.tmp %TEMP%\1f.tmp %TEMP%\20.tmp %TEMP%\21.tmp %TEMP%\22.tmp %TEMP%\22.tmp

Dr.Web vxCube will also provide you with the list of files created by the malware. Attackers are known to repeatedly encrypt malware so that its new iteration will avoid being detected by an



anti-virus. However, files within the encrypted container usually remain unchanged. If you also use a CERT solution, you can add the files to the list of possible signs of infection.

In conclusion, you will be presented with a list of the remote hosts that the malware was trying to reach. Those are most probably command and control servers, and it's a good idea to add them to the black list.

Created files [50]	Files and dumps [29]			Q
Path		SHA1	Detected	
%HOMEPATH%\start menu\pro	ograms\startup\yellnyglxu8.exe	c1c6d7fa967d4e95d8b61ae8c21a66c3f87cae28	Trojan.Carberp.647	<u>+</u>
%TEMP%\1.tmp		c1c6d7fa967d4e95d8b61ae8c21a66c3f87cae28	Trojan.Carberp.647	<u>+</u>
%TEMP%\10.tmp		cc33461f7147042c14d739ba7dc1916e6ccc8139	-	<u>+</u>
%TEMP%\11.tmp		e4eb14f7a950a30bc632446a9c9b418837378aac	-	<u>+</u>
%TEMP%\12.tmp		7cf3366c68e402eb3678046fe97651a586044560	-	<u>+</u>
%TEMP%\13.tmp		f683eb85535e34c41e5bf5da535d9dcc4aefe8b2	-	<u>+</u>
%TEMP%\14.tmp		08fe9ff1fe9b8fd237adedb10d65fb0447b91fe5	-	<u>+</u>
%TEMP%\15.tmp		a98e4be7f72f32b0ce5da60e59d2f6256d78bf04	-	<u>+</u>
%TEMP%\16.tmp		3127dbe44b75c673c24f9ad63675ff91cd9c6321	-	<u>+</u>
%TEMP%\19.tmp		3cf1eb1003a5342fd0f3495b67ff9bb90c855413	-	<u>+</u>
2 3 4 5 Next page			1–10 of 50	10 🗸
Protocol	<ul> <li>Address</li> </ul>	Application level data		
10	rucainost:80			
1P	10calhost:80			

In the **Office Control** section, you can add the discovered rogue hosts to the black list. **!** Select the **Everyone** group to block all protected hosts from accessing the malicious nodes.



## Anti-virus Network > Everyone > Windows > Office Control 😭

▼ Selected objects	General User-defined		si 🕼	\$
🗀 Everyone	Everyone. Custom settings are specified.			
Seneral     Statistics     Statistics     Configuration     Permissions     Task Scheduler     Installing components     Update restrictions     Connection settings     Dr.Web Agent for UNIX     Windows	Q Maninistrators Guests Users	General White list Black and white lists You can use white and black lists to allow or block access to specified web sites. White list	<u>.</u>	^ ^
Vindows     Scanner     SpIDer Guard for workstations     SpIDer Guard for servers     Office Control     Dr.Web Agent     Dr.Web for Microsoft Outlook		Black lat 谷 😚		



Doctor Web 2003–2019

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040 Tel.: +7 (495) 789–45–87 Fax: +7 (495) 789–45–97

https://www.drweb.com | https://free.drweb.com | https://ru.av-desk.com | https://curenet.drweb.com