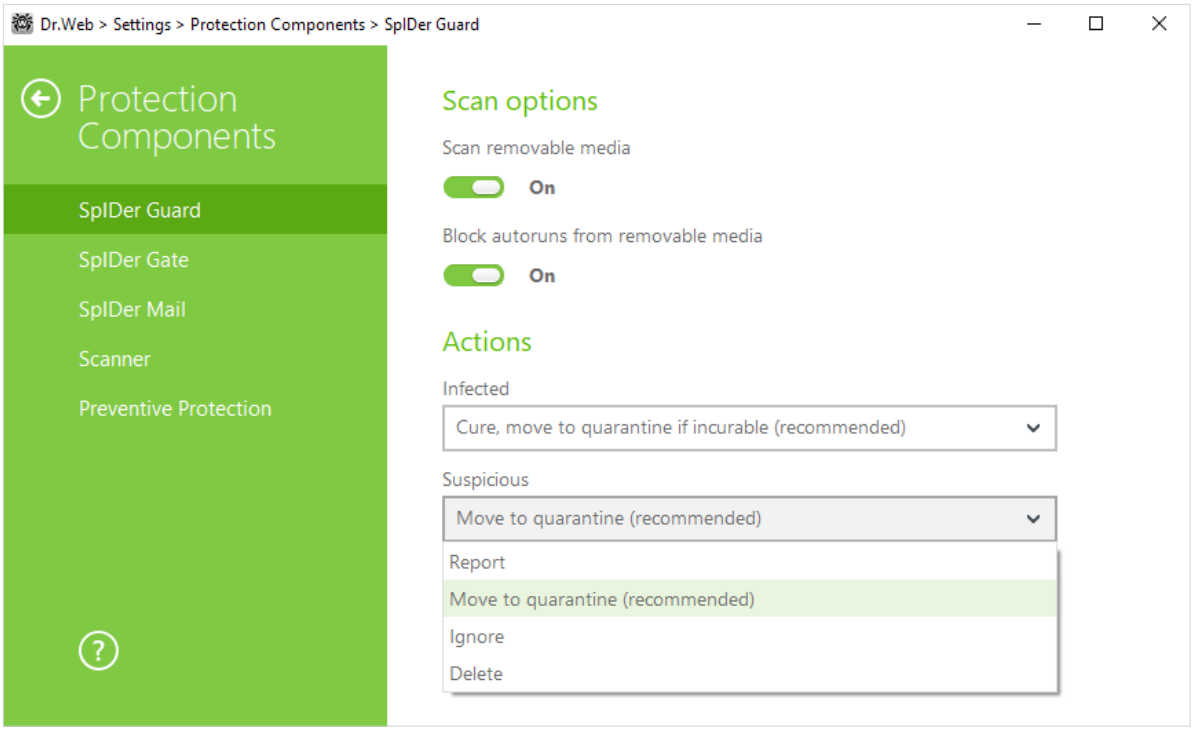
Dr.WEB®
since 1992

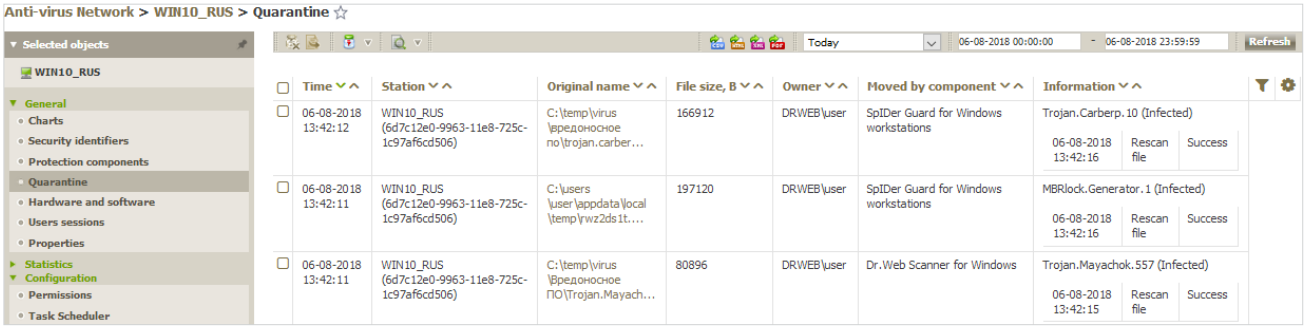
How Dr.Web vxCube can assist system administrators in their work

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

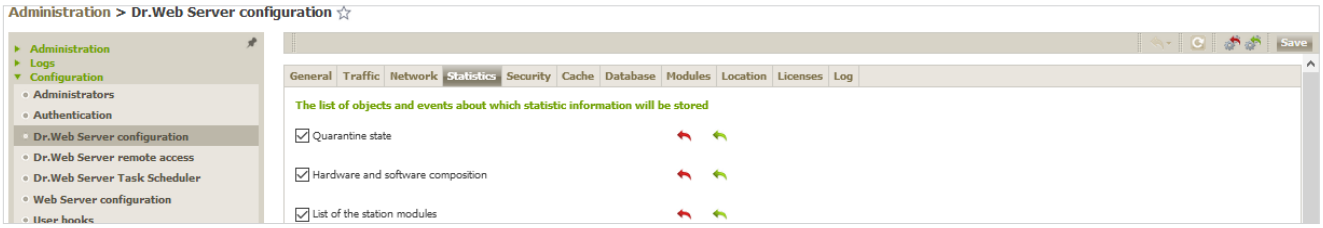
As they go about their work, system administrators encounter more than Trojans and viruses. Sometimes it's hard for them to tell at first glance whether a file is actually malicious. The anti-virus may flag it as suspicious. As a rule, files of this kind are moved by default to the quarantine. You can 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** → **Quarantine**). Use the filter to specify the desired period of time and to find the file you need to examine.

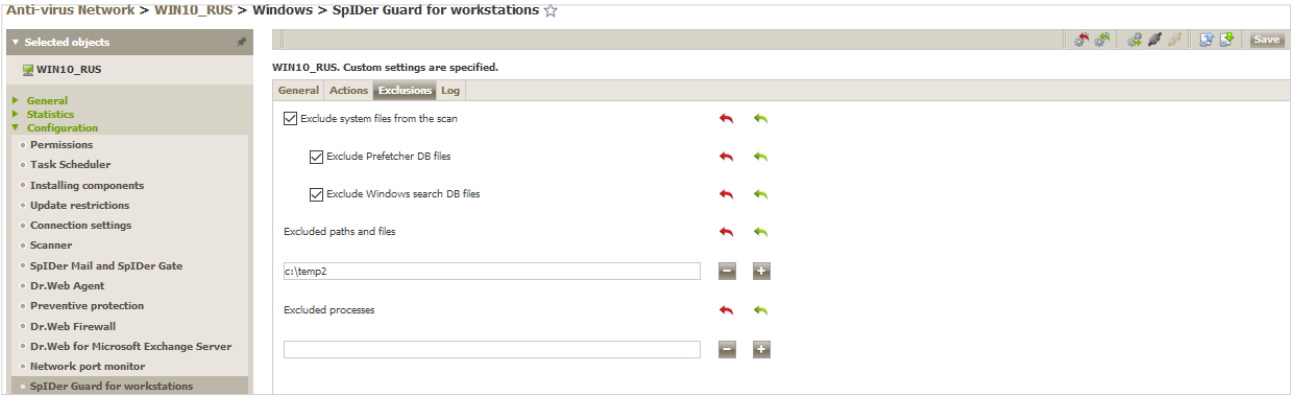


If the **Quarantine** item is not available in the **Anti-virus network menu**, go to **Administration** → **Dr.Web Server Configuration**. In the **Statistics** tab, tick the box **Quarantine state**.

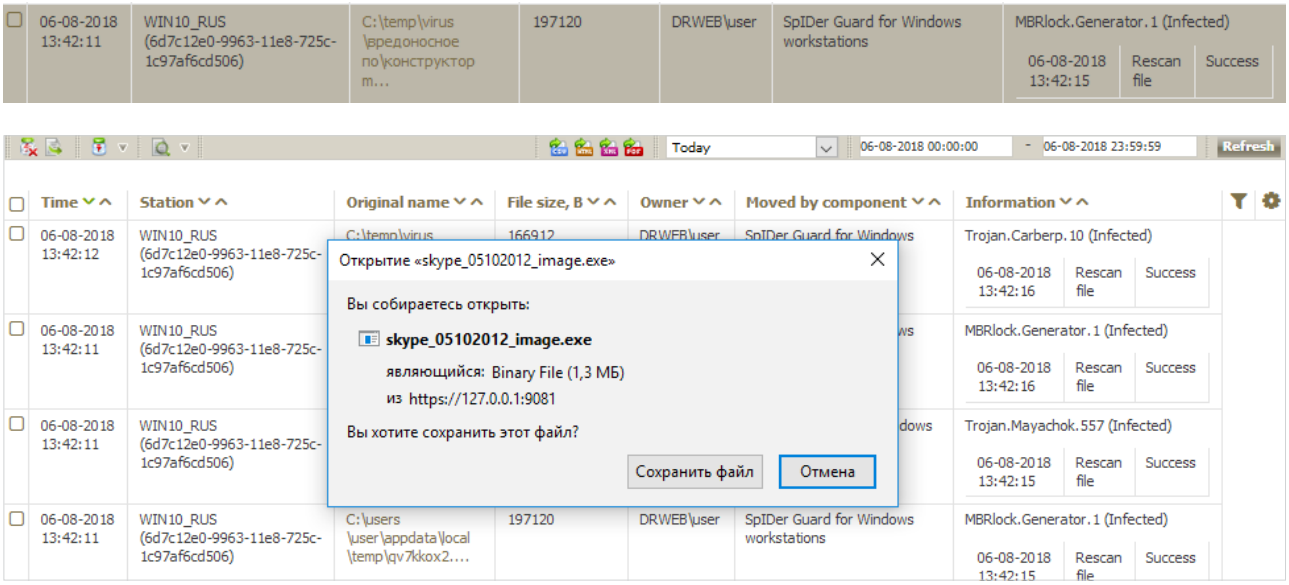


To examine a quarantined file, you must download it to a computer. Because the file is suspicious, the anti-virus protecting the PC will prevent the file from being saved on the hard drive. Disabling the anti-virus is a bad idea. Instead, select the host on which the file is to be saved. In **Anti-virus 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.

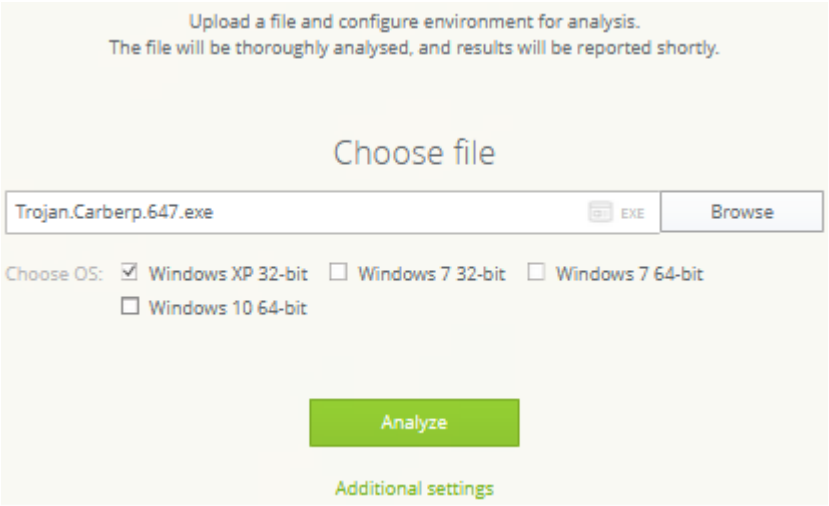
! It is not recommended to add your download folder to the exclusions list. Instead, create a separate directory.



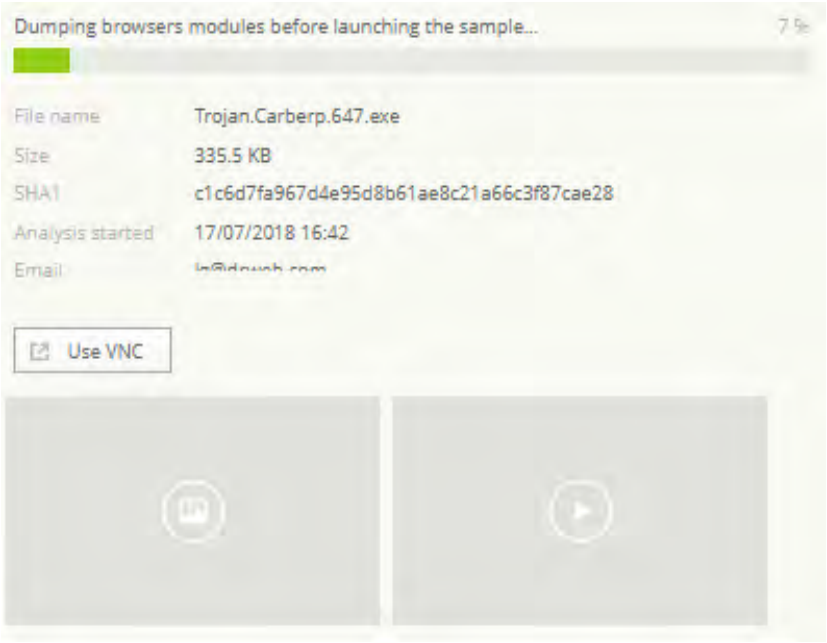
Once the folder is added to **Exclusions**, return to the **Quarantine** section. Select the file, click **Export**, and save the file to the appropriate directory.



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

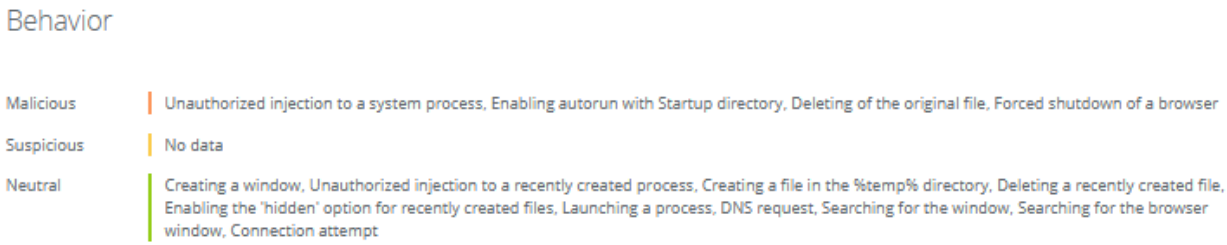


Wait while the file is being analysed.



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.



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.

Description

To ensure autorun and distribution:

Creates or modifies the following files:

- %HOMEPATH%\start menu\programs\startup\yellnyglxu8.exe

Malicious functions:

Injects code into the following system processes:

- <SYSTEM32>\svchost.exe

Terminates or attempts to terminate the following user processes:

- iexplore.exe
- firefox.exe

Modifies file system:

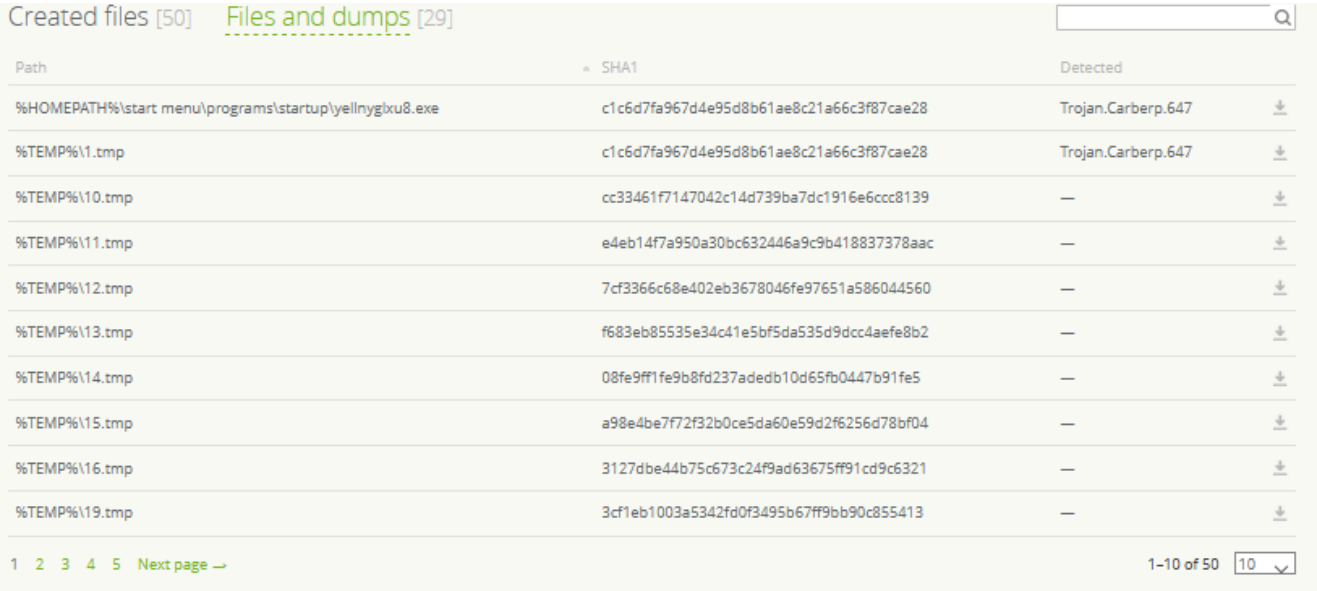
Creates the following files:

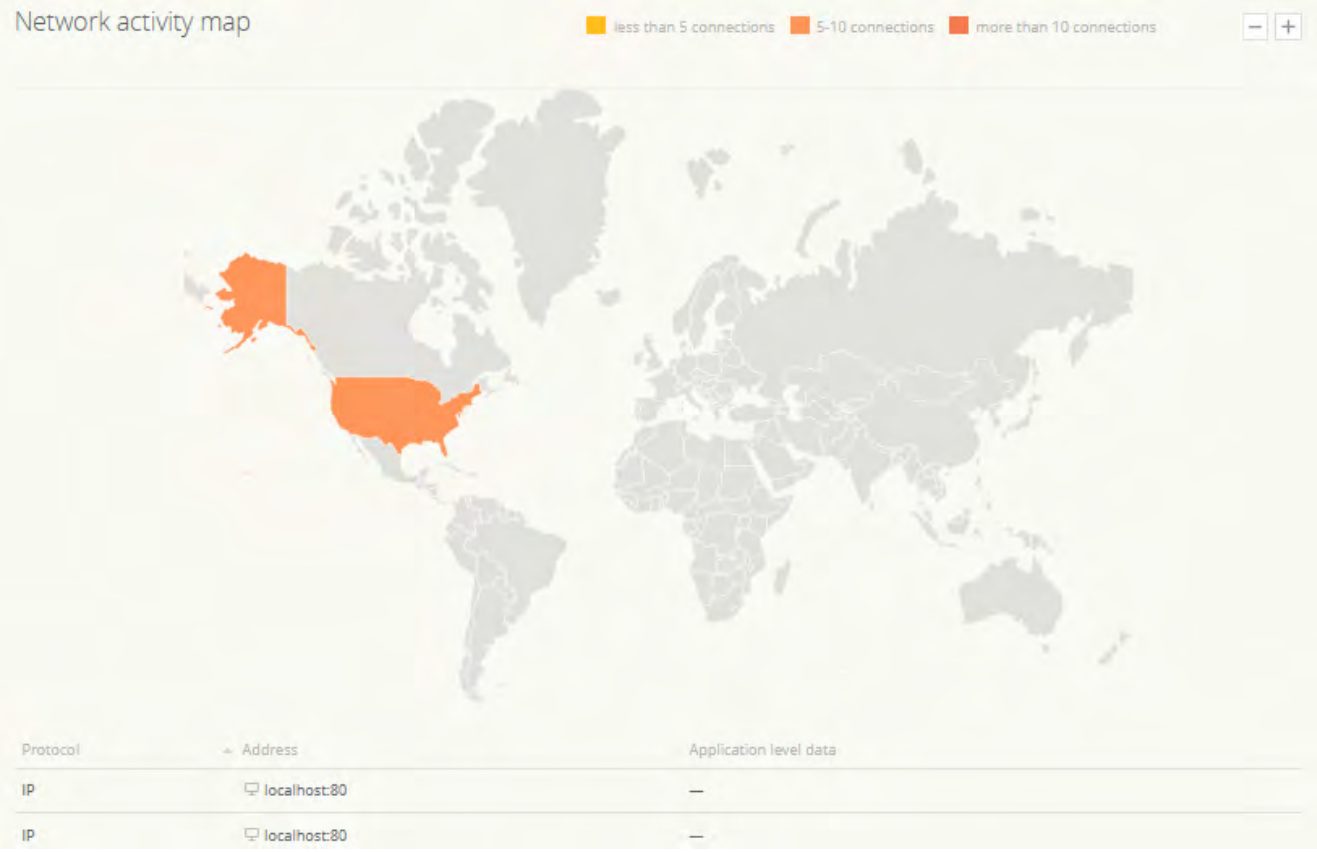
- %TEMP%\1.tmp
- %TEMP%\1f.tmp
- %TEMP%\20.tmp
- %TEMP%\21.tmp
- %TEMP%\22.tmp
- %TEMP%\23.tmp

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.

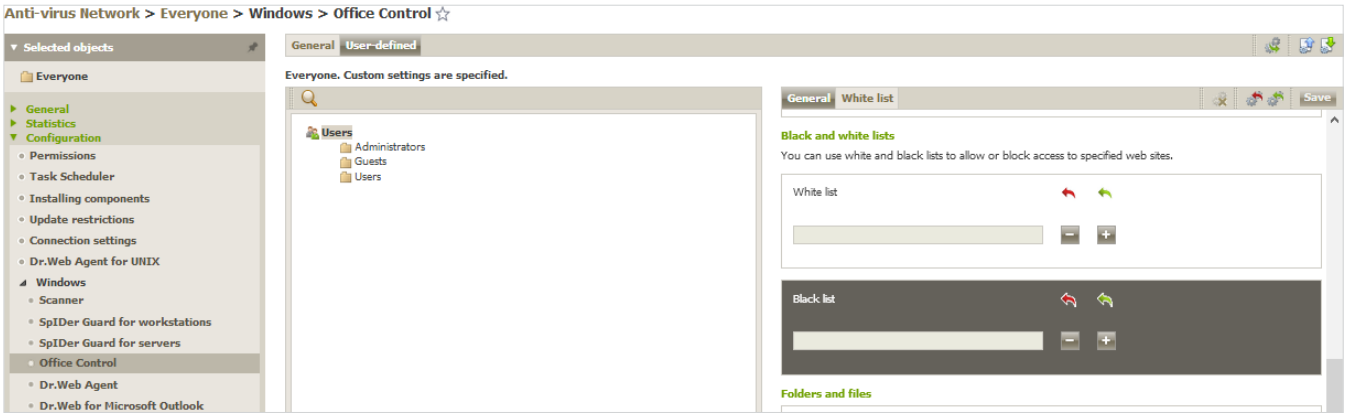
In conclusion, you will be presented with a list of the remote hosts that the malware was trying to reach. Those are most probably command and control servers, and it's a good idea to add them to the black list.





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.



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