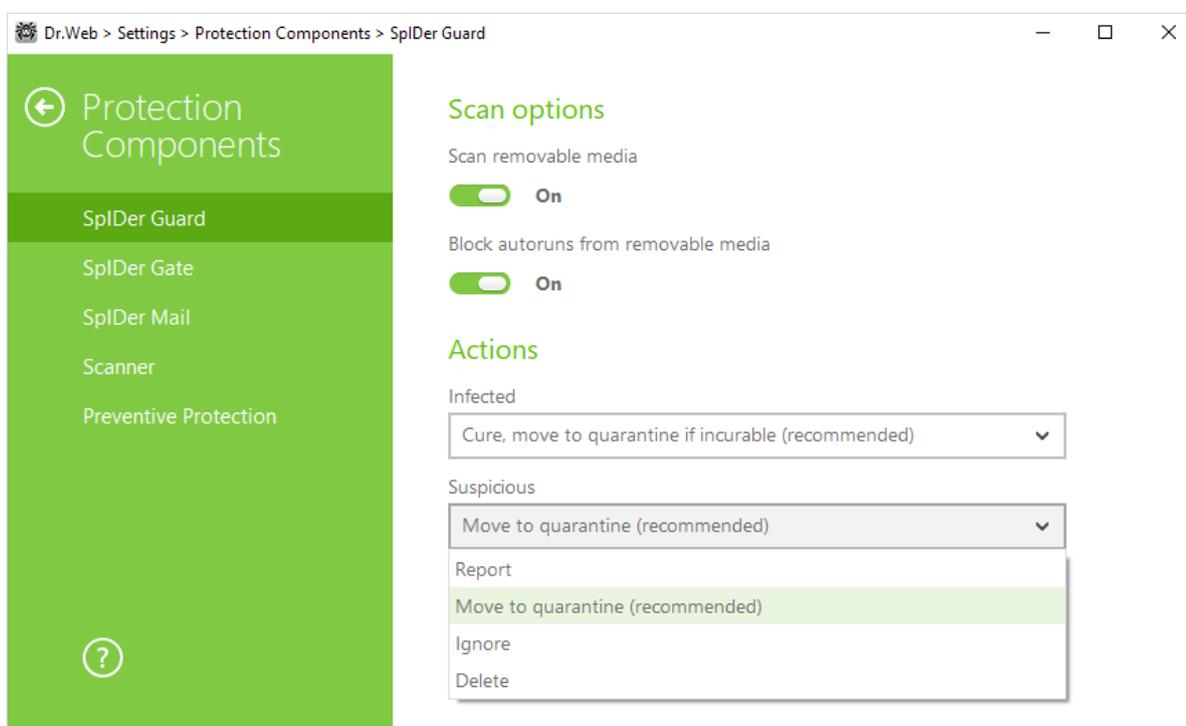


# How Dr.Web vxCube can assist system administrators in their work



## 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.



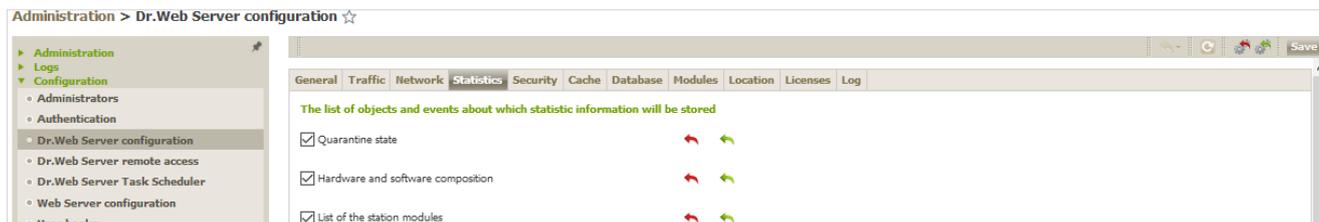
To analyse a suspicious file, open the Dr.Web Control Center and go to the quarantine section (**Administration** → **Quarantine**). Use the filter to specify the desired period of time and to find the file you need to examine.



The screenshot shows the 'Quarantine' section in the Dr.Web Control Center. It displays a table with columns for Time, Station, Original name, File size, Owner, Moved by component, and Information. The table contains three entries:

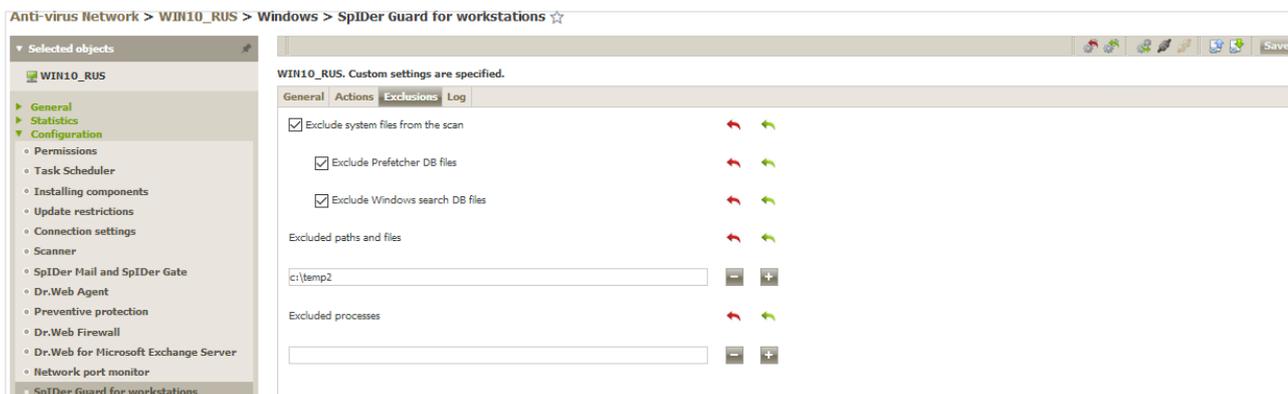
Time	Station	Original name	File size, B	Owner	Moved by component	Information
06-08-2018 13:42:12	WIN10_RUS (6d7c12e0-9963-11e8-725c-1c97af6cd506)	C:\temp\virus\редноное no)\trojan.carber...	166912	DRWEB\user	SplDer Guard for Windows workstations	Trojan.Carberp.10 (Infected) 06-08-2018 13:42:16 Rescan file Success
06-08-2018 13:42:11	WIN10_RUS (6d7c12e0-9963-11e8-725c-1c97af6cd506)	C:\users\user\appdata\local\temp\rvz2ds1t...	197120	DRWEB\user	SplDer Guard for Windows workstations	MBRlock.Generator.1 (Infected) 06-08-2018 13:42:16 Rescan file Success
06-08-2018 13:42:11	WIN10_RUS (6d7c12e0-9963-11e8-725c-1c97af6cd506)	C:\temp\virus\редноное ПИ)\Trojan.Mayach...	80896	DRWEB\user	Dr.Web Scanner for Windows	Trojan.Mayachok.557 (Infected) 06-08-2018 13:42:15 Rescan file Success

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**.



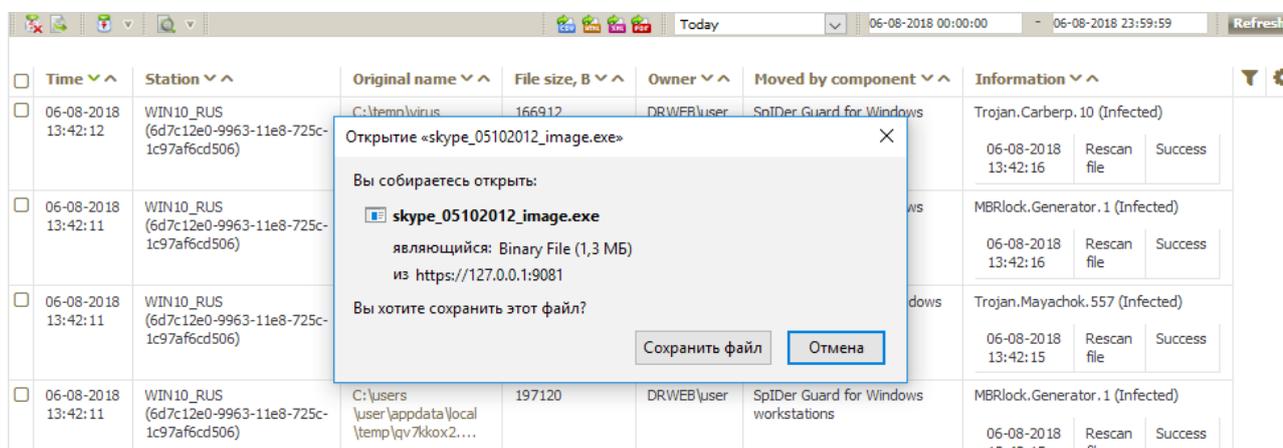
To examine a quarantined file, you must download it to a computer. Because the file is suspicious, the anti-virus protecting the PC will prevent the file from being saved on the hard drive. Disabling the anti-virus is a bad idea. Instead, select the host on which the file is to be saved. In **Anti-virus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

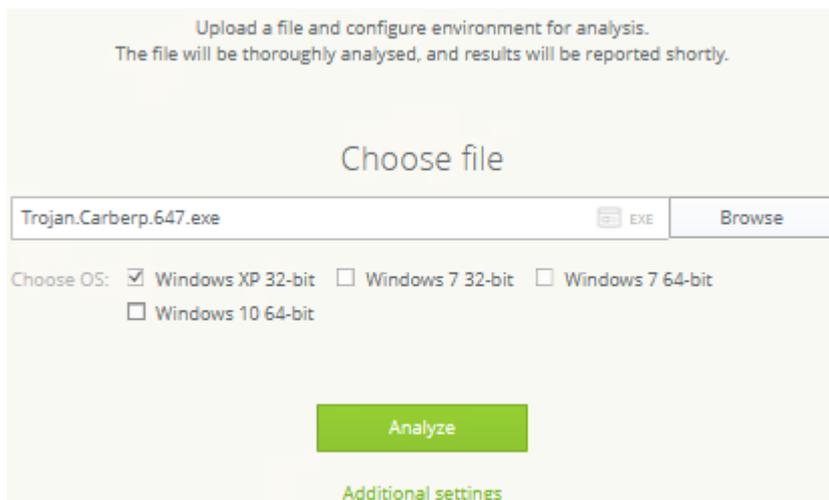


Once the folder is added to **Exclusions**, return to the **Quarantine** section. Select the file, click **Export**, and save the file to the appropriate directory.

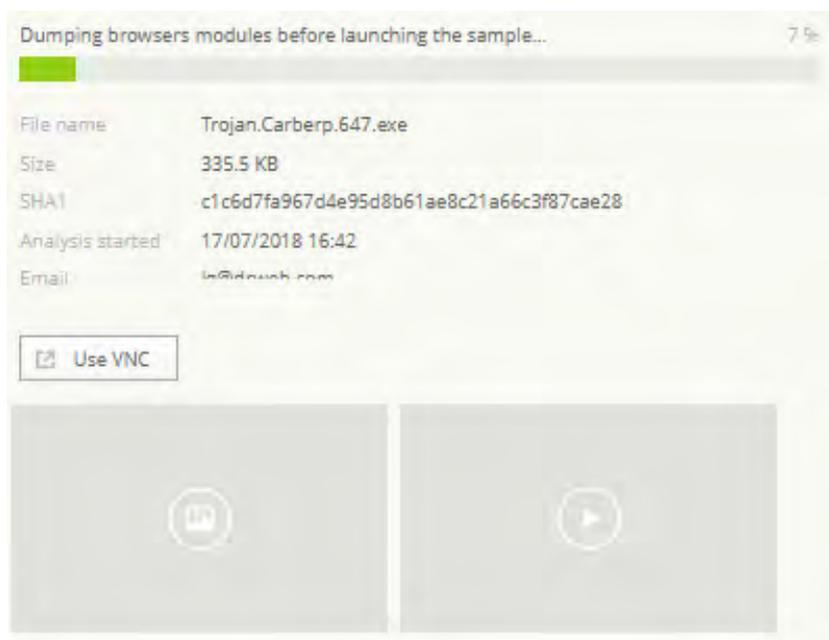
Time	Station	Original name	File size, B	Owner	Moved by component	Information
06-08-2018 13:42:11	WIN10_RUS (6d7c12e0-9963-11e8-725c-1c97af6cd506)	C:\temp\virus \редононое по\конструктор м...	197120	DRWEB\user	SpIDer Guard for Windows workstations	MBRlock.Generator.1 (Infected) 06-08-2018 13:42:15 Rescan file Success



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



Wait while the file is being analysed.



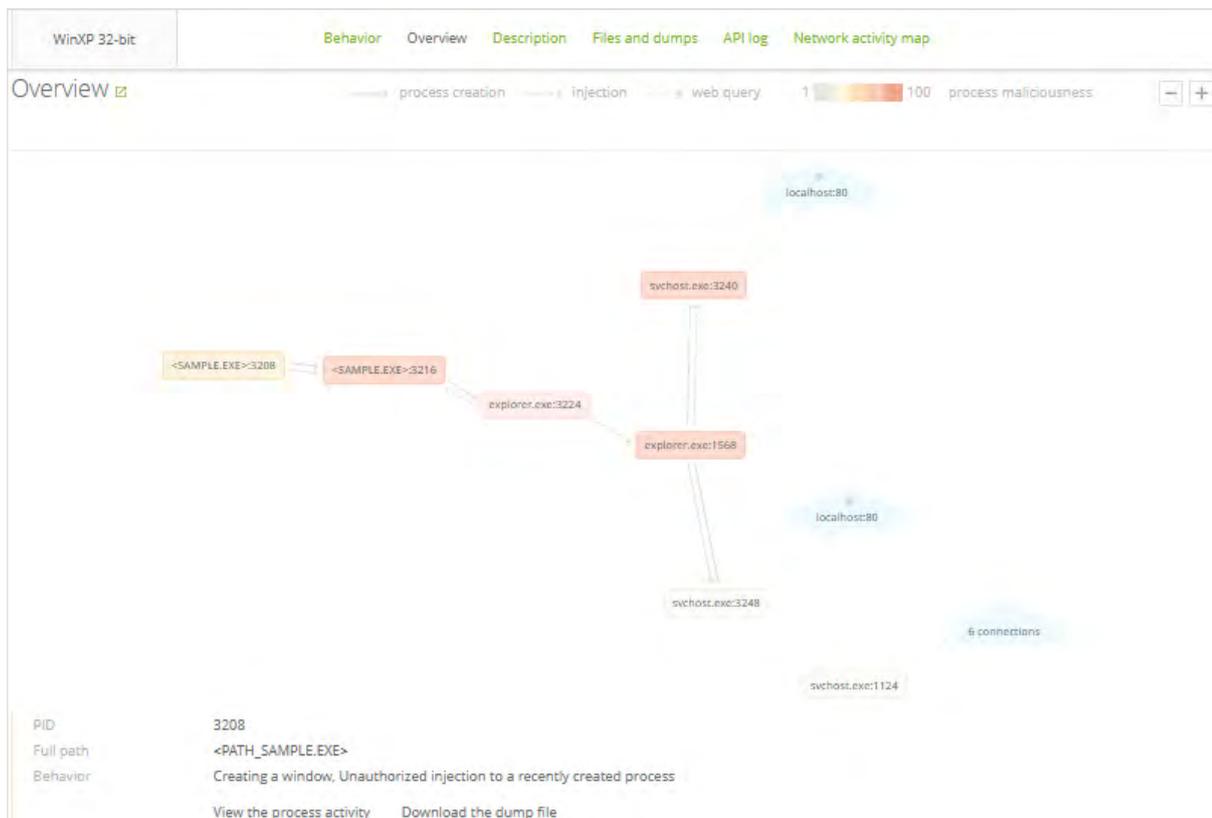
In some cases, when the analysis is complete, you can watch a video showing what the malicious file has been doing in the system.

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

### 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.



## 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

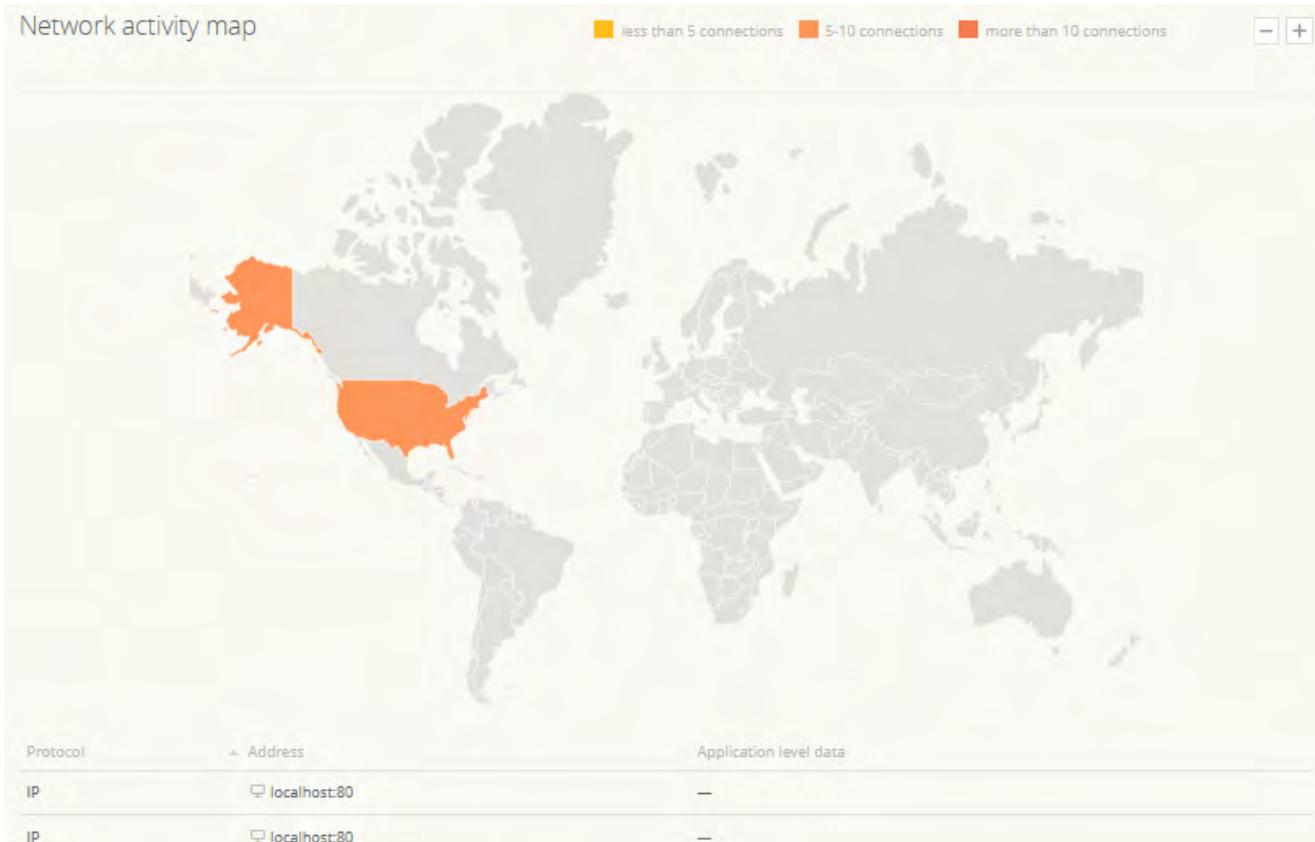
anti-virus. However, files within the encrypted container usually remain unchanged. If you also use a CERT solution, you can add the files to the list of possible signs of infection.

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.

Created files [50] [Files and dumps \[29\]](#)

Path	SHA1	Detected	
%HOMEPATH%\start menu\programs\startup\yellnyglxu8.exe	c1c6d7fa967d4e95d8b61ae8c21a66c3f87cae28	Trojan.Carberp.647	↓
%TEMP%\1.tmp	c1c6d7fa967d4e95d8b61ae8c21a66c3f87cae28	Trojan.Carberp.647	↓
%TEMP%\10.tmp	cc33461f7147042c14d739ba7dc1916e6ccc8139	—	↓
%TEMP%\11.tmp	e4eb14f7a950a30bc632446a9c9b418837378aac	—	↓
%TEMP%\12.tmp	7cf3366c68e402eb3678046fe97651a586044560	—	↓
%TEMP%\13.tmp	f683eb85535e34c41e5bf5da535d9dcc4ae8b2	—	↓
%TEMP%\14.tmp	08fe9ff1fe9b8fd237adedb10d65fb0447b91fe5	—	↓
%TEMP%\15.tmp	a98e4be7f72f32b0ce5da60e59d2f6256d78bf04	—	↓
%TEMP%\16.tmp	3127dbe44b75c673c24f9ad63675ff91cd9c6321	—	↓
%TEMP%\19.tmp	3cf1eb1003a5342fd0f3495b67ff9bb90c855413	—	↓

1 2 3 4 5 Next page → 1-10 of 50 10



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.

