

CLAIMS

1. A server to determine malicious files in network traffic, the server comprising:

5 a communication module configured to receive the network traffic from a data communication network,

a filtering module configured to connect to the communication module to receive the captured network traffic from the communication module and to perform at least the following
10 operations:

retrieving a plurality of files from the received network traffic,

analyzing the specified retrieved files, ensuring detection of at least one suspicious file from the specified plurality of the files,

15 a system monitoring module configured to connect to the filtering module to receive the specified suspicious files from the filtering module and to perform at least the following operations:

running every received suspicious file in at least one virtual machine, characterized by a specified set of status parameters,

20 recording changes in the specified set of the status parameters of at least one specified virtual machine,

a processing module configured to connect to the system monitoring module to receive from the system monitoring module the recorded changes of the status parameters and to analyze
25 the resulting changes of the status parameters using a specified set of analysis rules, ensuring classification of the specified started file as a malicious file if the analyzed changes of the status parameters are characteristic for the malicious files.

2. The server of claim 1, wherein the communication module is additionally configured to
30 connect to at least one of the network traffic capturing devices included in the data communication network.

3. The server of claim 1, wherein, when analyzing the extracted files, the filtering module may check whether the format of each of these retrieved files is suspicious, ensuring that the file
35 being checked will be classified as a trusted file if its format is not suspicious or as a suspicious file if its format is suspicious.

4. The server of claim 3, wherein, when checking the format of each of the specified retrieved files to be suspicious, the filtering module performs at least the following operations:

identifying the format of each of the specified retrieved files,

receiving the data about the known harmful file formats,

5 determining coincidence of the identified format of each retrieved file with one of the known harmful file formats from the specified received data.

10 5. The server of claim 3, wherein, in response to retrieving a file with the suspicious format, the filtering module is additionally configured to determine whether there is a behavioral report for the retrieved file with the suspicious format.

6. The server of claim 5, wherein, if the behavioral report exists, the filtering module performs at least the following operations:

receiving the data on behavioral reports,

15 calculating the hash sum of each retrieved file,

determining correspondence of each retrieved file to one of the existing behavioral reports, by comparing the calculated hash sum of the retrieved file with the hash sums that identify the behavioral reports in the specified received data,.

20 7. The server of claim 5, wherein, in response to detection of the behavioral report for the retrieved file with the suspicious format, the filtering module is additionally configured to check whether the existing behavioral report is up-to-date, ensuring classification of the extracted file as a trusted file or as a malicious file if it is classifies as such file in the up-to-date behavioral report.

25 8. The server of claim 7, wherein, in response to the fact that the existing behavioral report is not up-to-date, the filtering module is additionally configured to check whether the analyzed file is signed with the trusted electronic signature, ensuring that the file being checked is classified as a trusted file if it is signed with the trusted electronic signature.

30 9. The server of claim 8, wherein, when checking whether the retrieved file has the digital signature, the filtering module performs at least the following operations:

identifying the electronic signature owner used to sign the retrieved file,

receiving the data about the trusted owners of the electronic signatures,

35 determining coincidence of the identified electronic signature owner with one of the trusted owners of electronic signatures from the specified received data.

10. The server of claim 8, wherein, in response to the fact that the retrieved file is not signed by the trusted electronic signature, the filtering module may be additionally configured to check whether the specified file is originated from the trusted data source, ensuring that the file being checked is classified as a trusted file if it was originated from the trusted data source.

5

11. The server of claim 10, wherein the filtering module during check of origination of the retrieved file performs at least the following operations:

determining the retrieved file source,

receiving the data about the trusted sources,

10 determining coincidence of the particular source of the analyzed file origination with one of the trusted data sources from the specified received data.

12. The server of claim 10, wherein, in response to the fact that the retrieved file does not originate from the trusted data source, the filtering module is additionally configured to check
15 whether the trusted file identifier is assigned to the specified file, ensuring that the file being checked is classified as a trusted file if it was assigned the trusted file identifier.

13. The server of claim 12, wherein the filtering module during a check whether the retrieved file has the trusted file identifier, performs at least the following operations:

20 calculating the hash sum of the retrieved file,

receiving the data about the trusted files, wherein each file is matched to the particular hash sum,

determining coincidence of the calculated hash sum of the analyzed file with the hash sum of one of the trusted files from the specified received data.

25

14. The server of claim 13, wherein, in response to the fact that the retrieved file has no trusted file identifier, the filtering module is additionally configured to send the retrieved file to the system monitoring module.

30 15. The server of claim 1, wherein, to run each suspicious file in the specified virtual machine, the system monitoring module is additionally configured to perform at least the following operations:

identifying at least one attribute of each suspicious received file,

35 receiving the data about the existing virtual machines, wherein each of the virtual machines is characterized by the specified set of the configuration attributes,

determining in the existing virtual machines from the specified received data the default virtual machine, wherein at least one configuration attribute from the specified set of the configuration attributes coincides with the specified identified attribute of the suspicious file,

starting the suspicious file in the identified default virtual machine, ensuring
5 identification of at least one more attribute of the started file and determining coincidence of one more specified identified attribute with at least one more of the specified configuration attributes of the default virtual machine,

if at least one more specified identified attribute of the started file does not match to at least one more specified configuration attribute of the default virtual machine, restarting the
10 suspicious file in yet another virtual machine from the existing virtual machines, wherein the specified configuration attributes of the existing virtual machine coincides with the specified attributes of the suspicious file.

16. The server of claim 1, wherein, when recording changes in the specified set of the status
15 parameters of at least one specified virtual machine, the system monitoring module traces these changes during the predetermined time period of 2–3 minutes.

17. The server of claim 16, wherein the system monitoring module is additionally configured to change the specified set of the status parameters of each virtual machine and/or to change the
20 specified set of the analysis rules.

18. The server of claim 1, wherein, in response to classifying the file running on at least one specified virtual machine as a malicious file, the server monitoring system module is additionally configured to issue an alert message, to block the malicious file, to block the
25 malicious file sources, to add the malicious file into the malicious file database and/or to create the behavioral report for the malicious file.

19. A method to determine malicious files in network traffic, the method executing in a server, the method comprising:

30 receiving the network traffic from a data communication network, using a communication module of the server,

retrieving a plurality of files from the received network traffic, using a filtering module of the
35 server,

analyzing the specified retrieved files, ensuring detection of at least one suspicious file from the specified plurality of the files, using the filtering module,

starting each received suspicious file in at least one virtual machine characterized by a specified set of status parameters, using a system monitoring module of the server,

recording changes in the specified set of the status parameters of at least one specified virtual machine, using the system monitoring module.

analyzing, using a processing module of the server, the received changes of the status parameters using a specified set of analysis rules, ensuring that the specified started file is classified as a malicious file if the analyzed status parameter changes are characteristic for the malicious files.

20. The method of claim 19, wherein the stage of receiving the network traffic from the data communication network includes connection, via the server communication module, to at least one of the network traffic capturing devices in the data communication network.

21. The method of claim 19, wherein the stage of analyzing the retrieved files comprises the check whether the format of each of these retrieved files is suspicious, ensuring that the file being checked will be classified as a trusted file if its format is not suspicious or as a suspicious file if its format is suspicious.

22. The method of claim 21, wherein the stage of checking the format of each of the specified retrieved files to be suspicious comprises at least following sub-stages:

identifying the format of each of the specified retrieved files,

receiving the data about the known harmful file formats,

determining coincidence of the identified format of each retrieved file with one of the known harmful file formats from the specified received data.

23. The method of claim 21, wherein, in response to the fact that the retrieved file format is suspicious, it is additionally determined if there is the behavioral report for the extracted file with the suspicious format.

24. The method of claim 23, wherein the stage of detecting the behavioral report presence in the comprises receiving data about the behavioral reports, calculating the hash sum of each extracted file, and determining correspondence of each extracted file to one of the available

behavioral reports, by comparing the calculated hash sum of the extracted file with the hash sums identifying the behavioral reports in the specified received data.

25. The method of claim 23, wherein, in response to the fact that there is the behavioral report for the retrieved file with the suspicious format, it is additionally checked whether the existing behavioral report is up-to-date, ensuring classification of the retrieved file as a trusted file or as a malicious file if it is classifies as such file in the up-to-date behavioral report.

26. The method of claim 25, wherein the existing behavioral report is not up-to-date, the filtering module is additionally used to check whether the analyzed file is signed with the trusted electronic signature, ensuring that the file being checked is classified as a trusted file if it is signed with the trusted electronic signature.

27. The method of claim 26, wherein the stage of check whether the retrieved file has the trusted electronic digital signature comprises at least following sub-stages:
identifying the electronic signature owner used to sign the retrieved file,
receiving the data about the trusted owners of the electronic signatures,
determining coincidence of the identified electronic signature owner with one of the trusted owners of electronic signatures from the specified received data.

28. The method of claim 26, wherein, in response to the fact that the retrieved file is not signed with the trusted electronic signature, the server filtering module is additionally used to check whether the specified file is received from the trusted data source, ensuring that the file being checked is classified as a trusted file if it is originated from the trusted data source.

29. The method of claim 26, wherein the stage of checking origination of the retrieved file comprises at least following sub-stages:
determining the retrieved file source,
receiving the data about the trusted sources,
determining coincidence of the particular source of the analyzed file origination with one of the trusted data sources from the specified received data.

30. The method of claim 28, wherein, in response to the fact that the retrieved file does not originate from the trusted data source, the server filtering module is additionally used to check whether the trusted file identifier is assigned to the specified file, ensuring that the file being checked is classified as a trusted file if it is assigned the trusted file identifier.

31. The method of claim 30, wherein the stage of check whether the retrieved file has the trusted file identifier comprises at least following sub-stages:

calculating the hash sum of the retrieved file,

receiving the data about the trusted files, wherein each file is matched to the particular

5 hash sum,

determining coincidence of the calculated hash sum of the analyzed file with the hash sum of one of the trusted files from the specified received data.

32. The method of claim 30, wherein, in response to the fact that the received file has no
10 trusted file identifier, the server filtering module is additionally used to send the retrieved file to the system monitoring module.

33. The method of claim 19, wherein the stage of running each suspicious file in the virtual machine comprises at least following sub-stages:

15 identifying at least one attribute of each suspicious received file,

receiving the data about the existing virtual machines, wherein each of the virtual machines is characterized by the specified set of the configuration attributes,

determining in the existing virtual machines from the specified received data the default virtual machine, wherein at least one configuration attribute from the specified set of the
20 configuration attributes coincides with the specified identified attribute of the suspicious file,

starting the suspicious file in the identified default virtual machine, ensuring identification of at least one more attribute of the started file and determining coincidence of one more specified identified attribute with at least one more of the specified configuration attributes of the default virtual machine,

25 if at least one more specified identified attribute of the started file does not match to at least one more specified configuration attribute of the default virtual machine, restarting the suspicious file in yet another virtual machine from the existing virtual machines, wherein the specified configuration attributes of the existing virtual machine coincides with the specified attributes of the suspicious file.

30

34. The method of claim 33, wherein the stage of recording changes in the specified set of the status parameters of at least one virtual machine includes tracing by system monitoring module the specified changes during the specified time period of 2–3 minutes.

35 35. The method of claim 19, wherein the server system monitoring module is additionally configured to change the specified set of the status parameters of each virtual machine and/or to change the specified set of the analysis rules.

36. The method of claim 19, wherein, in response to classifying the file analyzed in the server processing module as a malicious file, the server processing module is used to issue an alert message, to block the malicious file, to block the malicious file sources, to add the malicious
5 file into the malicious file database and/or to create the behavioral report for the malicious file.

37. The method of claim 19, wherein each of the specified virtual machines is additionally configured by installing an operating system of the required architecture, choosing the operating system locale language, installing the necessary software and/or configuring the
10 installed software.

38. A computer-readable medium for long-term data storing that stores computer-readable instructions that, when executed by the server processor, cause execution of the method stages according to any of claims 19-37.

15