Claims

1. A decentralized malware check method, the method executed in a computer device having access to a distributed register and a transaction pool that are implemented in a peer-to-peer network, the method comprising:

   receiving input data related to a potentially malware, the potentially malware comprising an executable file;

   checking the potentially malware based on the received data related to the potentially malware;

   adding check parameters and at least one result of the potentially malware check into the transaction pool;

   receiving results of a distributed check of the potentially malware from a set of peer-to-peer network computer devices;

   determining a harmfulness parameter based on the results of the distributed check of the potentially malware received from the set of peer-to-peer network computer devices;

   identifying the malware in response to the harmfulness parameter of the potentially malware exceeding a predetermined threshold value; and

   storing the identified malware and associated data related to the identified malware received during execution of the method in the distributed register.

2. The method of claim 1, wherein the input data is received from at least one of the following sources: computer devices in the peer-to-peer network, at least one client device, a pre-formed database, a remote server, computer-readable media.

3. The method of claim 1, wherein the input data contains at least one pointing to the potentially malware.

4. The method of claim 1, wherein the input data additionally contains at least one of the following:
   malware signature;
   malware attribution data.

5. The method of claim 1, wherein the input data is received at least partially in a hashed form.

6. The method of claim 1, wherein at least a portion of the input data is hashed in response to the fact that at least the specified portion of the input data is received in a non-hashed form.

7. The method of claim 1, wherein, after receiving the input data, at least a portion of additional input data relating to this malware is extracted from at least one additional source accessible to the computer device.

8. The method of claim 7, wherein the check of the potentially malware is executed taking into account the additional input data related to this potentially malware.

9. The method of claim 1, wherein the potentially malware check is executed using a machine-learning algorithm.

10. The method of claim 9, wherein the training sample of the machine-learning algorithm is additionally updated in accordance with the confirmed results.

11. The method of claim 1, wherein the potentially malware is checked in an automated way.

12. The method of claim 11, wherein the potentially malware is checked manually.

13. The method of claim 1, wherein the potentially malware check based on the data related to this potentially malware comprises at least one of the following:

    determining harmfulness of the potentially malware;

    validating the signature of the potentially malware;

    identification of data on attribution of the potentially malware.

14. The method of claim 13, wherein the data on attribution of a potentially malware is determined on the basis of the data that is related to the potentially malware and received at least from one of the following sources:

    the received input data;

    the distributed register;

    a malicious resource database.

15. The method of claim 13, wherein the data on attribution of a potentially malware is determined using the machine-learning algorithm.

16. The method of claim 1, wherein, at the step of adding the check parameters and results of at least one result of check of potentially malware into the transaction pool, additional data that is related to the potentially malware and received from at least one additional source, available to a computer device is also entered into the transaction pool.

17. The method of claim 1, wherein the harmfulness parameter is determined based on the results of the distributed potentially malware check, which are received from the set of peer-to-peer network computer devices, and on at least one of the following parameters:

    a number of the peer-to-peer network computer devices that downloaded data about the potentially malware;

    a reputation of the peer-to-peer network computer devices that downloaded data about the potentially malware;

    a number of the peer-to-peer network computer devices that confirmed the result of the check of the potentially malware;

    a reputation of the peer-to-peer network computer devices that confirmed the result of the check of the potentially malware.

18. The method of claim 1, wherein, after storing the identified malware in the distributed register, tokens are charged to the computer devices of the distributed peer-to-peer network where the check results were obtained, corresponding to the harmfulness parameter determined based on the results of the distributed check of the potentially malware received from the set of the peer-to-peer network computer devices.

19. The method of claim 1, wherein, after storing the identified malware and the associated data related to the identified malware received during execution of the method in the distributed register, the identified malware and the associated data related to the identified malware received during the method execution are additionally saved in at least one malware database accessible to the computer device.

20. The method of claim 1, wherein, after storing the identified malware and the associated data related to the identified malware received during execution of the method in the distributed register, the identified malware and the associated data

related to the identified malware received during the method execution are additionally saved into the learning set of the machine-learning algorithm.

21. A computer device for decentralized malware check, having access to a distributed register and a transaction pool that are implemented on the basis of a peer-to-peer network, the computer device contains a communication interface and at least one computer processor functionally connected to the communication interface, the computer processor configured to:

receive input data related to a potentially malware, the potentially malware comprising an executable file;

check the potentially malware based on the received data related to the potentially malware;

add check parameters and at least one result of the potentially malware check into the transaction pool;

receive results of a distributed check of the potentially malware from a set of peer-to-peer network computer devices;

determine a harmfulness parameter based on the results of the distributed check of the potentially malware received from the set of peer-to-peer network computer devices;

identify the malware in response to the harmfulness parameter of the potentially malware exceeding the predetermined threshold value;

store the identified malware and associated data related to the identified malware received during execution of the method in the distributed register.

22. The device of claim 21, wherein the processor is additionally configured to receive input data from at least one of the following sources: computer devices in the peer-to-peer network, at least one client device, a pre-formed database, a remote server, computer-readable media.

23. The device of claim 21, wherein the processor is additionally configured to receive input data comprising at least one pointing to the potentially malware.

24. The device of claim 21, wherein the processor is additionally configured to receive input data that additionally comprise at least one of the following:

the malware signature;

the malware attribution data.

25. The device of claim 21, wherein the processor is additionally configured to receive input data at least partially in a hashed form.

26. The device of claim 21, wherein the processor is additionally configured to hash at least a portion of the input data in response to the fact that at least the specified portion of the input data is received in a non-hashed form.

27. The device of claim 21, wherein at least one additional source is accessible and the processor is additionally configured to retrieve at least a part of additional input data related to this malware from the at least one additional source.

28. The device of claim 27, wherein the processor is additionally configured to check the potentially malware taking into account the additional input data related to this potentially malware.

29. The device of claim 21, wherein the processor is additionally configured to check the potentially malware using a machine-learning algorithm.

30. The device of claim 29, wherein the processor is additionally configured to update a training sample of the machine-learning algorithm in accordance with the confirmed results.

31. The device of claim 21, wherein the processor is additionally configured to check the potentially malware in an automated way.

32. The device of claim 31, wherein the processor is additionally configured to get results of the check of the potentially malware in a manual way.

33. The device of claim 21, wherein the processor is additionally configured to check the potentially malware based on the received data related to this potentially malware and to execute one of the following:

    determining harmfulness of the potentially malware;
    validating the signature of the potentially malware;
    identification of data on attribution of the potentially malware.

34. The device of claim 33, wherein the processor is additionally configured to determine the data on attribution of a potentially malware based on the data that

are related to the potentially malware and received at least from one of the following sources:

the received input data;

the distributed register;

a malicious resource database.

35. The device of claim 33, wherein the processor is additionally configured to determine the data on attribution of the potentially malware using a model based on neural networks.

36. The device of claim 21, wherein the processor is additionally configured to add into the transaction pool the additional data that is related to the potentially malware and received at least from one additional source available to the computer device.

37. The device of claim 21, wherein the processor is additionally configured to determine the harmfulness parameter based on the results of the distributed potentially malware check, the results are received from the set of peer-to-peer network computer devices, and on at least one of the following parameters:

a number of the peer-to-peer network computer devices that downloaded data about the potentially malware;

a reputation of the peer-to-peer network computer devices that downloaded data about the potentially malware;

a number of the peer-to-peer network computer devices that confirmed the result of the check of the potentially malware;

a reputation of the peer-to-peer network computer devices that confirmed the result of the check of the potentially malware.

38. The device of claim 21, wherein the processor is additionally configured to store the identified malware and the associated data related to the identified malware into at least one malware database accessible to the computer device.

39. The device of claim 21, wherein the processor is additionally configured to store the identified malware and the associated data related to the identified malware into a learning set of a machine-learning algorithm.