

WHAT IS CLAIMED IS:

1. A computer implemented method for detection and prevention of an attempt at establishment of a network connection for malicious communication, comprising:

detecting a connection establishment process for establishing a network connection, the connection establishment process initiated by an application executed by a processor of a client terminal;

obtaining from a call stack of the application records of at least one stack trace of the initiating application managed at the client terminal;

detecting a trial to establish a malicious communication for using the network connection for malicious activity based on an analysis of the application records; and

blocking establishment of the network connection when the analysis detects the trial to establish the malicious communication based on the network connection.

2. The method of claim 1, wherein the analysis comprises an analysis of flow-data including the at least one stack trace and at least one member of the group consisting of: thread data, module data, and process data related to the connection establishment.

3. The method of claim 1, further comprising:

gathering, at each respective client, data related to the at least one stack trace and/or flow-data; and

transmitting, from each respective client to a central server, the data related to the at least one stack trace;

wherein the analysis is performed by the central server;

wherein data related to the at least one stack trace includes dynamic code.

4. The method of claim 1, further comprising permitting the connection establishment process to activate the network connection when the trial to establish the malicious communication when the network connection is not detected.
5. The method of claim 1, wherein the at least one stack trace is collected during the connection establishment executed according to a transmission control protocol (TCP) of the internet protocol suite for initiation of the connection establishment process.
6. The method of claim 1, wherein the at least one stack trace includes at least one sequence of multiple stack traces obtained at multiple points during the connection establishment process, and the analysis comprises matching the multiple stack traces to flow-data analysis representing the trial to establish the malicious communication.
7. The method of claim 1, wherein said analysis comprises analyzing the records of the at least one stack trace for at least one of an unknown module and a blacklisted or whitelisted module, representing infection of the initiating application.

8. The method of claim 1, wherein said analysis comprises analyzing the at least one stack trace for connection establishment flow-data analysis used by uninfected applications designated as valid at a central server performing the analysis.
9. The method of claim 1, wherein said analysis comprises a comparison of at least one stack trace with connection establishment stack flow-data analysis expected to be generated by the application when the application has not been infected with injected code that initiates the trial to establish the malicious activity/communication.
10. A system for detection of an attempt at establishment of a network connection for malicious communication, comprising:
 - at least one gateway configured to:
 - receive at least one stack trace of an application executed by a processor of a client terminal during a connection establishment process for establishing a network connection with a network based server;
 - obtaining from a call stack of the application records of the at least one stack trace;
 - determine a presence or absence of a trial to establish a malicious communication for using the network connection for malicious activity based on an analysis of the application records; and
 - generate a signal representing the trial to establish the malicious communication using the network connection.

11. The system of claim 10, wherein the at least one gateway resides at a remote server communicating with the client terminal over a network.
12. The system of claim 10, wherein the at least one gateway is a software module residing at the client terminal.
13. The system of claim 10, further comprising:
 - an endpoint module for installation at the client terminal, configured to:
 - detect an initiation of establishment of the network connection by the application;
 - transmit the at least one stack trace and/or flow-data to the gateway;
 - receive the signal from the gateway; and
 - block the connection establishment process to prevent activation of the network connection based on the received signal.
14. The system of claim 10, further comprising:
 - a management server in communication with the at least one gateway, the management server configured to collect the signal generated by the at least one gateway for each network connection request related to each client.
15. The system of claim 14, wherein the management server further includes a user interface configured to allow a user to perform at least one member of the group consisting of: review the generated signals, manage the generated signals, centrally control the configuration of the at least one gateway, centrally control the configuration of at least one client terminal communicating with the at least one gateway, monitor status of the at least one gateway, and monitor status of at least one client terminal communicating with the at least one gateway.

16. The system of claim 10, wherein the connection establishment process is managed by an application programming interface that represents a local end point for the network connection.

17. The system of claim 10, further comprising updating the at least one gateway with a stack flow-data analysis associated with the identified attempt at establishing the network connection for the malicious communication, to identify similar stack flow-data analysis from other client terminals.

18. The system of claim 10, wherein the at least one gateway is further configured to:

receive at least one stack trace of the application when the network connection is active; and

analyze records in the at least one stack trace to monitor for post connection establishment malicious activity using the active network connection.

19. The system of claim 10, wherein the at least one gateway is further configured to:

receive a plurality of at least one flow-data from each of a plurality of clients; and

analyze the plurality of at least one flow-data to detect a coordinated attack.

20. A computer program product for detection of an attempt at establishment of a network connection for malicious activity, the computer program product comprising:

at least one non-transitory computer-readable storage medium, and program instructions stored on at least one of the at least one storage mediums, the program instructions comprising:

program instructions for detecting a connection establishment process for establishing a network connection, the connection establishment process initiated by an application executed by a processor of a client terminal;

program instructions for obtaining from a call stack of the application records of at least one stack trace of the initiating application which is managed at the client terminal;

program instructions for detecting a trial to establish a malicious communication wherein the network connection is used for malicious activity based on an analysis of the application records; and

program instructions for blocking establishment of the network connection when the analysis detects the trial to establish the malicious communication based on the network connection.