

WHAT IS CLAIMED IS:

1. A method for authenticating an attempt at establishment of a network connection by allowed code, comprising:

providing a dataset having a plurality of previously observed stack trace templates each representing a stack trace pattern prevailing in stack traces recorded by monitoring a plurality of stacks of a plurality of clients executing an allowed code during a connection establishment process for establishing network connections related to the allowed code;

receiving a new stack trace recorded during a new connection establishment process for a new network connection by a new client;

measuring a similarity between the new stack trace and the plurality of stack trace templates to identify a match to a stack trace template;

evaluating the matched stack trace template for a predefined rule requirement; and

updating a rule-set database with the matched stack trace template to authenticate new network connection establishments associated with stack templates matching the matched stack trace template;

wherein evaluating the matched stack trace template comprises: incrementing a value of a counter indicative of a number of previous stack trace template matches from different clients, and evaluating the value against the predefined rule requirement of a number of matches.

2. The method of claim 1, wherein the plurality of stack trace templates are designated as representing suspicious malicious behavior of the allowed code.

3. The method of claim 1, wherein the plurality of stack trace templates and the new stack trace include context data collected in association with the stack trace of the allowed code, and the similarity is measured according to the context data.

4. The method of claim 3, wherein the context data includes an event ID and/or host name; wherein the context data includes at least one member selected from the

group consisting of: similar operating system running at the respective client, similar allowed application, similar stack trace data by different allowed applications, and similar protocols to establish the network connection.

5. The method of claim 1, wherein the different clients are part of a same designated group.

6. The method of claim 1, wherein evaluating the matched stack trace template for the predefined rule requirement is performed when the matched stack trace template and the new stack trace are associated with different clients.

7. The method of claim 1, further comprising:
analyzing the new stack trace, to designate the network connection as being suspicious of being related to malicious code; and
further comprises re-designating the suspicion of being related to malicious code as being related to the allowed code.

8. The method of claim 7, wherein the suspicion of being related to malicious code is triggered by a new allowed code installed on the new client displaying malicious-like behavior.

9. The method of claim 7, wherein the allowed code represents a false positive identification by incorrectly triggering the identification of suspicious of being related to malicious code.

10. The method of claim 7, wherein the stack trace associated with the authenticated new network connection is matched to at least one stack trace template associated with an attempt at establishing the network connection for malicious communication.

11. The method of claim 1, wherein the new stack trace and the plurality of stack trace templates further comprise flow-data including at least one member selected from the group consisting of: processes, modules, and threads.

12. The method of claim 1, wherein the plurality of stack trace templates are based on authorized installation of similar allowed code on a plurality of the clients within a predefined period of time.

13. The method of claim 1, wherein the predefined requirement is at least one of:
 selected to prevent or reduce false positive connection blocking of allowed network connections by the allowed code, and represents a tolerance level for false positive connection blocking of allowed network connections.

14. A system for authenticating an attempt at establishment of a network connection by allowed code, comprising:

a dataset having a plurality of previously observed stack trace templates each representing a stack trace pattern prevailing in stack traces recorded by monitoring a plurality of stacks of a plurality of clients executing an allowed code during a connection establishment process for establishing network connections related to the allowed code; and

at least one event management server including a code implementable by a processor of the at least one event management server to:

receive a new stack trace recorded at a certain new client of a plurality of clients during a new connection establishment process for a new network connection by the certain new client;

measure a similarity between the new stack trace and the plurality of stack trace templates to identify a match to a stack template;

evaluate the matched stack trace template for a predefined requirement by:

incrementing a value of a counter indicative of a number of previous stack trace template matches from different clients, and

evaluating the value against the predefined rule requirement of a number of matches; and

update a rule-set database with the matched stack trace template to authenticate new network connection establishments associated with stack templates matching the matched stack trace template.

15. The system of claim 14, further comprising at least one gateway server in communication with the event management server and with at least one of the plurality of client terminals, the at least one gateway server including a code implementable by a processor of the at least one gateways server to:

analyze the new stack trace to designate the new network connection as being suspicious of being related to malicious code;

transmit the new stack trace to the event management server for analysis;

receive the updated rule-set database; and

allow connection establishment of the new network connection.

16. The system of claim 14, wherein the at least one event management server is in communication with a plurality of gateway servers, wherein each respective gateway server is in communication with at least one client of the plurality of clients, each respective gateway is includes a code implementable by a processor of each respective gateway to:

receive, from the new client, the new stack trace;

analyze the new stack trace to determine a presence or absence of a suspected trial to establish a malicious communication wherein the network connection is used for malicious activity;

detect an attempt at establishing the network connection for the malicious communication when the new stack trace is correlated with malicious data; and

generate a message representing the suspected trial to establish the malicious communication using the network connection; and

the code of the event management server is implementable to receive the message from each respective gateway server, and perform the measuring, evaluating and updating to re-designate the new network connection as

representing an allowed network connection, to prevent or reduce blocking of false positive network connections by allowed code that appear malicious to the respective gateway.

17. The system of claim 16, wherein the certain new client further comprises an allowed application associated with the allowed code that including a code implementable by a processor of the new client to trigger the suspicious of being related to malicious code identification.

18. The system of claim 14, wherein the allowed code is at least one of: installed as injected code within an application, the injected code being associated with stack data similar to stack data associated with malicious injected code and configured with high level permission to establish a network connection in a manner similar to high level permission obtained by malicious code.

19. The system of claim 14, further comprising a client module for installation at each respective client, the client module including a code implementable by a processor of the respective client to:

- identify a newly installed application at the respective client; and

- analyze the newly installed application to identify a trial to establish a connection for malicious communication by the newly installed application.

20. A computer program product for authenticating an attempt at establishment of a network connection by allowed code, the computer program product comprising:

- program instructions to provide a dataset having a plurality of previously observed stack trace templates each representing a stack trace pattern prevailing in stack traces recorded by monitoring a plurality of stacks of a plurality of clients executing an allowed code during a connection establishment process for establishing network connections related to the allowed code;

- program instructions to receive a new stack trace recorded during a new connection establishment process for a new network connection by a new client;

program instructions to measure a similarity between the new stack trace and the plurality of stack trace templates to identify a match to a stack trace template;

program instructions to evaluate the matched stack trace template for a predefined rule requirement; and

program instructions to update a rule-set database with the matched stack trace template to authenticate new network connection establishments associated with stack templates matching the matched stack trace template;

wherein evaluating the matched stack trace template comprises: incrementing a value of a counter indicative of a number of previous stack trace template matches from different clients, and evaluating the value against the predefined rule requirement of a number of matches.