

CLAIMS

What is claimed is:

1. A URL attack detection method, wherein the method comprises:

extracting a set of features of multiple dimensions from information comprised in
 5 a plurality of URL access request samples, wherein none of the plurality of URL
 access request samples are labeled;

constructing a plurality of training samples based on the set of features;

obtaining a URL attack detection model by using the plurality of training
 samples and based on an Isolation Forest machine learning algorithm, comprising:

10 obtaining M training sample subsets from the plurality of training
 samples; and

constructing M random binary trees, wherein each one of the M
 random binary trees corresponds to a particular training sample subset of the
 M training sample subsets, and wherein constructing a random binary tree
 15 comprises:

while a stopping condition is not satisfied:

selecting a classification feature randomly from
 dimensions of features as a root node,

20 selecting a classification threshold value randomly
 between the maximum value of the classification feature and
 the minimum value of the classification feature among all
 training samples comprised in the particular training sample
 subset,

25 determining a first set of training samples comprised in
 the particular training sample subset whose values of the
 classification feature are greater than or equal to the
 classification threshold value as a first leaf node of the root
 node and determining a second set of training samples
 comprised in the particular training sample subset whose values
 30 of the classification feature are less than the classification
 threshold value as a second leaf node of the root node, and

setting the first set of training samples or the second set

of training samples as the particular training sample subset;

extracting features of multiple dimensions from information comprised in a URL access request;

obtaining a risk score of the URL access request by providing the features to the
5 URL attack detection model for prediction calculation, wherein the URL attack detection model is a machine learning model obtained through training based on the Isolation Forest machine learning algorithm; and

determining, based on the risk score, that the URL access request is a URL attack request.

10

2. The method according to claim 1, wherein obtaining the risk score of the URL access request comprises:

constructing a prediction sample based on the extracted features;

traversing each random binary tree from a root node based on a value of each
15 feature in the prediction sample to find a leaf node corresponding to the prediction sample; and

calculating an average value of path depths of found leaf nodes in all the random binary trees, and normalizing the average value to obtain the risk score of the URL access request.

20

3. The method according to claim 1, wherein the information comprises at least one of domain name information or a URL parameter; and the features of multiple dimensions comprise features extracted from the domain name information comprised in at least one of the URL access request or features extracted from the URL
25 parameter comprised in the URL access request.

4. The method according to claim 3, wherein the features comprise a combination of multiple of the following features: a total quantity of characters, a total quantity of letters, a total quantity of numbers, a total quantity of symbols, a
30 quantity of different characters, a quantity of different letters, a quantity of different numbers, and a quantity of different symbols.

5. A URL attack detection apparatus, wherein the apparatus comprises:

a first extraction module, configured to extract a set of features of multiple

dimensions from information comprised in a plurality of URL access request samples, wherein none of the plurality of URL access request samples are labeled;

a construction module, configured to construct a plurality of training samples based on the set of features;

5 a training module, configured to obtain a URL attack detection model by using the plurality of training samples and based on an Isolation Forest machine learning algorithm, comprising:

obtaining M training sample subsets from the plurality of training samples; and

10 constructing M random binary trees, wherein each one of the M random binary trees corresponds to a particular training sample subset of the M training sample subsets, and wherein constructing a random binary tree comprises:

while a stopping condition is not satisfied:

15 selecting a classification feature randomly from dimensions of features as a root node,

selecting a classification threshold value randomly between the maximum value of the classification feature and the minimum value of the classification feature among all training samples comprised in the particular training sample subset,

20 determining a first set of training samples comprised in the particular training sample subset whose values of the classification feature are greater than or equal to the classification threshold value as a first leaf node of the root node and determining a second set of training samples comprised in the particular training sample subset whose values of the classification feature are less than the classification threshold value as a second leaf node of the root node, and

30 setting the first set of training samples or the second set of training samples as the particular training sample subset;

a second extraction module, configured to extract features of multiple dimensions from information comprised in a URL access request;

a calculation module, configured to obtain a risk score of the URL access request

by providing the features to the URL attack detection model for prediction calculation, wherein the URL attack detection model is a machine learning model obtained through training based on the Isolation Forest machine learning algorithm; and

5 a determining module, configured to determine, based on the risk score, that the URL access request is a URL attack request.

6. The apparatus according to claim 5, wherein the calculation module is configured to:

construct a prediction sample based on the extracted features;

10 traverse each random binary tree from a root node based on a value of each feature in the prediction sample to find a leaf node corresponding to the prediction sample; and

calculate an average value of path depths of found leaf nodes in all the random binary trees, and normalize the average value to obtain the risk score of the URL
15 access request.

7. The apparatus according to claim 5, wherein the information comprises at least one of domain name information or a URL parameter; and the features of multiple dimensions comprise features extracted from the domain name information comprised
20 in at least one of the URL access request or features extracted from the URL parameter comprised in the URL access request.

8. The apparatus according to claim 7, wherein the features comprise a combination of multiple of the following features: a total quantity of characters, a
25 total quantity of letters, a total quantity of numbers, a total quantity of symbols, a quantity of different characters, a quantity of different letters, a quantity of different numbers, and a quantity of different symbols.

9. An electronic device, comprising:

30 at least one processor; and

a memory, configured to store a machine executable instruction, wherein

by reading and executing a machine executable instruction that corresponds to control logic of URL attack detection and that is stored in the memory, the at least one processor is prompted to:

extract a set of features of multiple dimensions from information comprised in a plurality of URL access request samples, wherein none of the plurality of URL access request samples are labeled;

construct a plurality of training samples based on the set of features;

5 obtain a URL attack detection model by using the plurality of training samples and based on an Isolation Forest machine learning algorithm, comprising:

obtaining M training sample subsets from the plurality of training samples; and

10 constructing M random binary trees, wherein each one of the M random binary trees corresponds to a particular training sample subset of the M training sample subsets, and wherein constructing a random binary tree comprises:

while a stopping condition is not satisfied:

15 selecting a classification feature randomly from dimensions of features as a root node,
selecting a classification threshold value randomly between the maximum value of the classification feature and the minimum value of the classification feature among all training samples comprised in the particular training sample subset,

20

determining a first set of training samples comprised in the particular training sample subset whose values of the classification feature are greater than or equal to the classification threshold value as a first leaf node of the root node and determining a second set of training samples comprised in the particular training sample subset whose values of the classification feature are less than the classification threshold value as a second leaf node of the root node, and

25

setting the first set of training samples or the second set of training samples as the particular training sample subset;

30

extract features of multiple dimensions from information comprised in a URL access request;

obtain a risk score of the URL access request by providing the features to the URL attack detection model for prediction calculation, wherein the URL

attack detection model is a machine learning model obtained through training based on the Isolation Forest machine learning algorithm; and

determine, based on the risk score, that the URL access request is a URL attack request.