

CLAIMS

1. A method for detecting a domain name family of a botnet, comprising:

obtaining suspicious domain names;

building a domain name space-time correlation graph based on correlations between the suspicious domain names in different dimensions, wherein in the domain name space-time correlation graph, each suspicious domain name is taken as a node, an edge is formed between two domain names having at least one correlation, and the correlation between the two domain names is taken as an attribute value of the edge; and

determining domain names that are closely correlated in the domain name space-time correlation graph according to a determination index of a compactness of each node in graph computing, and taking a set of the corresponding domain names as the domain name family of the botnet;

wherein determining the domain names that are closely correlated in the domain name space-time correlation graph according to the determination index of the compactness of each node in graph computing comprises: removing an abnormal subgraph and an abnormal node in the domain name space-time correlation graph, and determining the domain names that are closely correlated in the domain name space-time correlation graph;

wherein removing the abnormal subgraph and the abnormal node in the domain name space-time correlation graph comprises:

decomposing the domain name space-time correlation graph into subgraphs composed of a plurality of connected components according to connectivity, and removing an abnormal subgraph that does not meet a preset first connectivity index;

dividing remaining subgraphs after removing the abnormal subgraph by using a community discovery algorithm to obtain communities composed of a plurality of connected components, and removing an abnormal community that does not meet a preset second connectivity index; and

measuring degree of importance of each node in remaining communities after removing the abnormal community by using a web page ranking algorithm, and removing a potential abnormal node with low degree of importance.

2. The method for detecting the domain name family of the botnet according to claim 1, wherein determining the domain names that are closely correlated in the domain name space-time correlation graph according to the determination index of the compactness of each node in graph computing comprises:

determining the domain names that are closely correlated in the domain name space-time correlation graph according to sparseness and average clustering degree.

3. The method for detecting the domain name family of the botnet according to claim 1, wherein the correlations in different dimensions comprises any combination of the following characteristics:

similarity in grammatical features of the domain names, similarity in correlations between the domain names and a virus, similarity in IP addresses resolved from the domain names, and similarity in access traffics of the domain names.

4. The method for detecting the domain name family of the botnet according to any one of claims 1 to 3, wherein after taking the set of the corresponding domain names as the domain name family of the botnet, the method further comprises:

analyzing a family characteristic of the domain name family of the botnet, and performing security detection on an application scenario based on the analyzed family characteristic.

5. The method for detecting the domain name family of the botnet according to claim 4, wherein after taking the set of the corresponding domain names as the domain name family of the botnet, the method further comprises:

determining whether a new domain name belongs to the domain name family of the botnet by determining correlation between the new domain name and a known domain name, to monitor variant and expansion of the domain name family of the botnet.

6. The method for detecting the domain name family of the botnet according to claim 1,

wherein building the domain name space-time correlation graph based on correlations between the suspicious domain names in different dimensions comprises:

expressing the correlation between the suspicious domain names in different dimensions in a form of a triple, wherein a correlation index in the triple includes a dimension of the correlation and similarity measure of two domain names in the dimension; and

building the domain name space-time correlation graph based on the triple by using a graph database.

7. The method for detecting the domain name family of the botnet according to claim 1, wherein the second connectivity index is more stringent than the first connectivity index in terms of connectivity indexes.

8. A device for detecting a domain name family of a botnet, comprising:

a domain name obtaining module configured to obtain suspicious domain names;

a correlation graph building module configured to build a domain name space-time correlation graph based on correlations between the suspicious domain names in different dimensions, wherein in the domain name space-time correlation graph, each suspicious domain name is taken as a node, an edge is formed between two domain names having at least one correlation, and the correlation between the two domain names is taken as an attribute value of the edge; and

a detection module configured to determine domain names that are closely correlated in the domain name space-time correlation graph according to a determination index of a compactness of each node in graph computing, and take a set of the corresponding domain names as the domain name family of the botnet;

wherein the detection module is configured to: remove an abnormal subgraph and an abnormal node in the domain name space-time correlation graph to determine the domain names that are closely correlated in the domain name space-time correlation graph;

wherein the detection module is configured to:

decompose the domain name space-time correlation graph into subgraphs composed of a

plurality of connected components according to connectivity, and remove an abnormal subgraph that does not meet a preset first connectivity index;

divide remaining subgraphs after removing the abnormal subgraph by using a community discovery algorithm to obtain communities composed of a plurality of connected components, and remove an abnormal community that does not meet a preset second connectivity index; and

measure degree of importance of each node in remaining communities after removing the abnormal community by using a web page ranking algorithm, and remove a potential abnormal node with low degree of importance.

9. The device for detecting the domain name family of the botnet according to claim 8, wherein the detection module is configured to:

determine the domain names that are closely correlated in the domain name space-time correlation graph according to sparseness and average clustering degree.

10. The device for detecting the domain name family of the botnet according to claim 8, wherein the correlations in different dimensions comprises any combination of the following characteristics:

similarity in grammatical features of the domain names, similarity in correlations between the domain names and a virus, similarity in IP addresses resolved from the domain names, and similarity in access traffics of the domain names.

11. The device for detecting the domain name family of the botnet according to any one of claims 8 to 10, wherein the device further comprises:

a security detection module configured to analyze, after taking the set of the corresponding domain names as the domain name family of the botnet, a family characteristic of the domain name family of the botnet, and perform security detection on an application scenario based on the analyzed family characteristic.

12. The device for detecting the domain name family of the botnet according to claim 11, wherein the device further comprises:

a monitoring module configured to determine, after taking the set of the corresponding

domain names as the domain name family of the botnet, whether a new domain name belongs to the domain name family of the botnet by determining correlation between the new domain name and a known domain name, to monitor variant and expansion of the domain name family of the botnet.

13. The device for detecting the domain name family of the botnet according to claim 8, wherein the correlation graph building module is configured to:

express the correlation between the suspicious domain names in different dimensions in a form of a triple, wherein a correlation index in the triple includes a dimension of the correlation and similarity measure of two domain names in the dimension; and

build the domain name space-time correlation graph based on the triple by using a graph database.

14. The device for detecting the domain name family of the botnet according to claim 8, wherein the second connectivity index is more stringent than the first connectivity index in terms of connectivity indexes.

15. An apparatus for detecting a domain name family of a botnet, comprising:

a memory configured to store a computer program; and

a processor configured to execute the computer program to implement steps of the method for detecting the domain name family of the botnet according to any one of claims 1 to 7.

16. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program that, when executed by a processor, implements steps of the method for detecting the domain name family of the botnet according to any one of claims 1 to 7.