CLAIMS

1. A computer-implementable method for malware or cybercriminal infrastructure detection, the method comprising:

• receiving a request comprising at least one infrastructure element and a tag that the infrastructure element belongs to a malware or cybercriminal;

• extracting from a database at least one parameter of the infrastructure element, at least one additional infrastructure element that is used by the same malware or cybercriminal as the infrastructure element, and at least one parameter of the at least one additional infrastructure element;

• analyzing the at least one infrastructure element, the at least one parameter of the infrastructure element, the additional infrastructure element, and the at least one parameter of the at least one additional infrastructure element;

• detecting, based on the analysis, statistical relationships between the at least one parameter of the infrastructure element and the at least one parameter of the at least one additional infrastructure element;

• creating rules of searching new infrastructure elements based on the detected statistical relationships;

• extracting new infrastructure elements from the database using the created rules;

• assigning tags corresponding to specific malwares or cybercriminals to the new elements, and storing the new elements and assigned tags in the database.

2. The method of claim 1, wherein the parameters of malware or cybercriminal infrastructure elements are at least one of:

- IP address;
- domain name;
- SSL certificate;
- server;
- web service;
- e-mail address;
- telephone number.

3. The method of claim 1, wherein the database is continuously updated with data obtained by Internet scanning.

4. The method of claim 3, wherein the Internet scanning is performed by at least one vulnerability scanner.

5. The method of claim 1, wherein conventional or common name of the malware or cybercriminal is used as the tag.

6. The method of claim 1, wherein the request comprising at least one infrastructure element is received from at least one of the following sources:

- sandbox;
- malware detonation platform;
- vulnerability scanner;
- honeypot;
- intrusion detection system;
- system of emergency response to cyber security incidents.

7. The method of claim 1, wherein the statistical relationships are detected by machine learning algorithms.

8. The method of claim 1, wherein the statistical relationship represents at least two parameters combined by at least one logic operation, wherein each of the parameters belongs to at least two different infrastructure elements.

9. The method of claim 1, wherein the created rules are stored and configured to receive rule updates.

10. A system for malware or cybercriminal infrastructure detection, the system comprising:

- a database module, the database module is configured to store infrastructure elements, parameters of infrastructure elements and tags that the infrastructure elements belong to malwares or cybercriminals;
- a request processing module, wherein the request processing module is configured to
    - receive a request comprising at least one infrastructure element and a tag that the infrastructure element belongs to a malware or cybercriminal;
    - extract from the request information about the malware or cybercriminal infrastructure element, and information that the infrastructure element belongs to the malware or cybercriminal;
- a data extraction module, wherein the data extraction module is configured to:
    - receive from the request processing module the infrastructure element, and the tag;
    - extract from the database at least one parameter of the infrastructure element, at least one additional infrastructure element that is used by the same malware or cybercriminal as the infrastructure element, and at least one parameter of the at least one additional infrastructure element;
    - extract new infrastructure elements from the database using a rule created in an analytical module;
    - assign tags corresponding to specific malwares or cybercriminals to the new infrastructure elements, and store the new elements and assigned tags in the database;
- the analytical module, the analytical module is configured to:

- analyze the at least one infrastructure element, the at least one parameter of the infrastructure element, the additional infrastructure element, and the at least one parameter of the additional infrastructure element;
- detect, based on the analysis, statistical relationships between the at least one parameter of the infrastructure element, and the at least one parameter of the at least one additional infrastructure element;
- create the rules of searching new infrastructure elements based on the detected statistical relationship.