TITLE

INFORMATIONAL SECURITY NETWORK FOR EXCHANGE OF RECORDED COMPUTER THREATS AND CONSECUTIVE INTERCEPTION OF VIRUSES AND OTHER COMPUTER ATTACKS ON THE USERS CONNECTED TO THIS NETWORK

FIELD OF THE INVENTION

This innovation belongs to the antivirus software. Specifically, it is part of the computer software for blocking detected computer viruses and other computer threats by means of network communication via exchange of information about detected threats in real time. The invention is also applicable to dynamic heuristic method of blocking computer viruses and other informational security threats by means of exchanging information about threats between users.

BACKGROUND OF THE INVENTION

Traditional methods of preventing virus infections and other cyber security threats currently employed by end-users of various electronic devices as a rule include the option to install a security system from a given software developer company therefor security is provided by the means of search of virus signatures in the database of that software developer.

Utilizing heuristic analysis methods for files with executable code are analyzed and decision is made regarding potential infection of the file. Standard signatures are not utilized during heuristic analysis. On a contrary heuristic module calculates it's decision based on previously developed algorithms that are not always streamlined and updated.

Code emulation allows for application to start in the emulated environment where operating system or processor is emulated. That way tested application is harmless to the system and potential threat could be detected by emulating software (emulator).

Behavioral analysis methods and technology allows evaluating not only single malware action but also a sequence of actions to increase efficiency of anti-virus software.

Although these measures could be sufficient for prevention of cyber threats for user's operating system and virus protection they are not sufficient for newly emerging viruses and threats. Virus protection often requires all above-mentioned measures to be updated regularly and promptly regardless of any particular protection software technical capabilities. Otherwise protection utilizing such software bears risks to be breached.

Cloud based anti-viruses is another example of providing cyber protection, they are able to provide security only in the proprietary developer's framework without inclusion of technologies from other developers.

There are cyber security service providers that are conducting virus checks utilizing anti-virus software from multiple original software developers. Results of such checks do not depend on single product capabilities. This approach produces more reliable threat detection. However it does not provide a real-time defense solution and requires manual download of every file through specific API or web form at the according web page.

Obviously, there is a need for effective real time solution that is able to provide cyber defense utilizing all relevant data available from many different cyber security software including anti-virus software producers. This invention is targeted to providing such a solution.

The aim of this invention is to create effective and efficient mean/system to neutralize computer virus and other cyber threats. Besides the aim of this invention is to create a mean for data exchange regarding already detected cyber threats in real time manner regardless of the type of the operating system or the type of end-user device.

The subject of the invention is development of cyber security threat prevention system. These and other goals of the invention will be obvious for relevant experts based on the description provided down below.

SUMMARY OF THE INVENTION

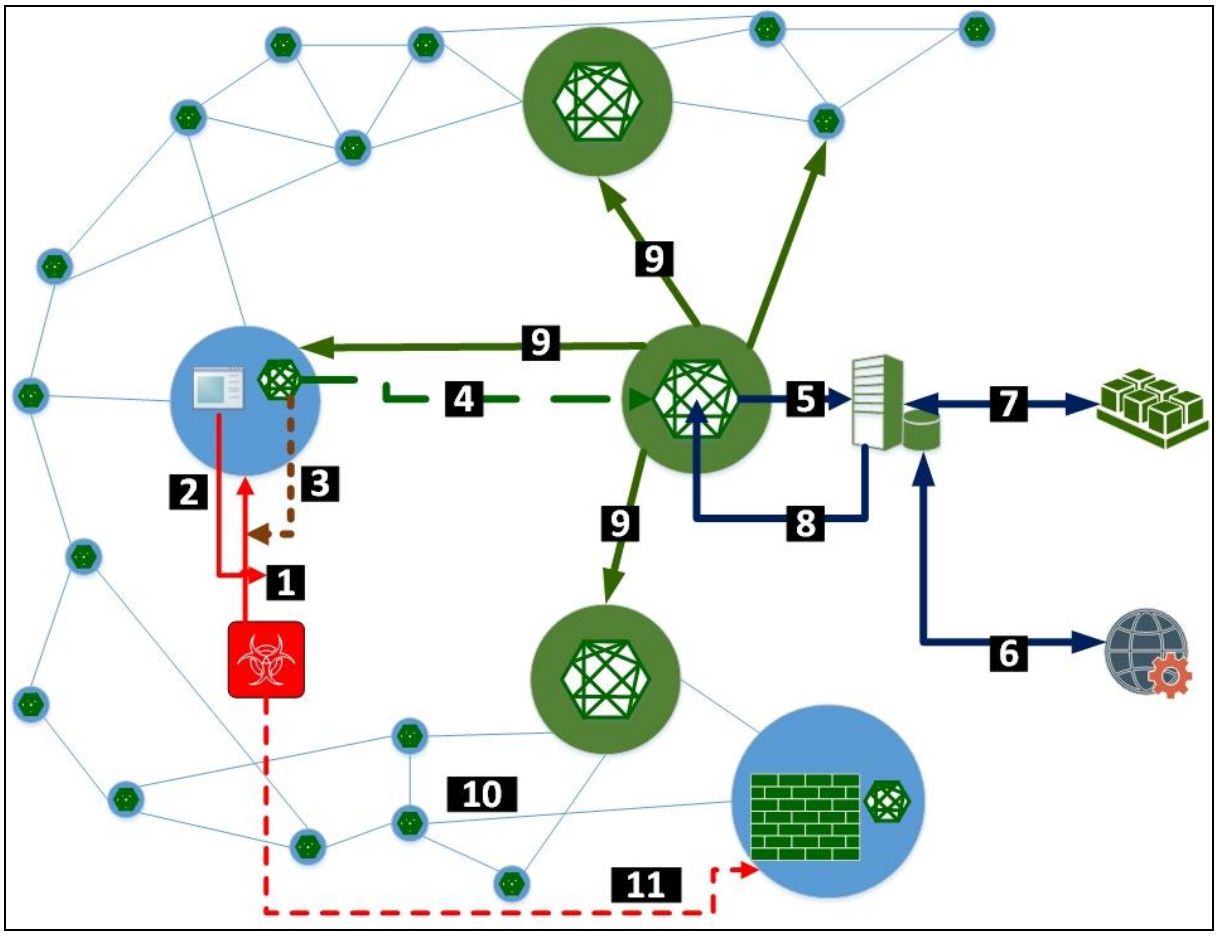
The mean and the system based on this invention presented as innovative concept for provision of preventive measures in cyber security on condition of suspected file/virus was detected by any of the cyber security systems or anti-virus software. The invention allows to delete or neutralize suspicions files, viruses, and cyber security threats regardless installed antivirus software at the particular endpoint. Also it is possible to operate without installed anti-virus or other cyber security system.

This is a network of informational security where each user connected to the network exchanges information about IT security incidents (viruses and any other computer threats) detected on his device with other users in real time in order to prevent an attack directed at any devices of users connected to the network. Users of the network agree to exchange such information about threats on their devices. Device threat detection is done by monitoring the response of alien protection systems installed on the user device. Protection system response is analyzed by the client program and other means of analysis that are located both on the user device and outside of it on other nodes of network. Following such analysis, users are notified of the threat. Users get such threat notification in form of a prepared packet of information via various communication tools with various network protocols in place. The source of notification can be

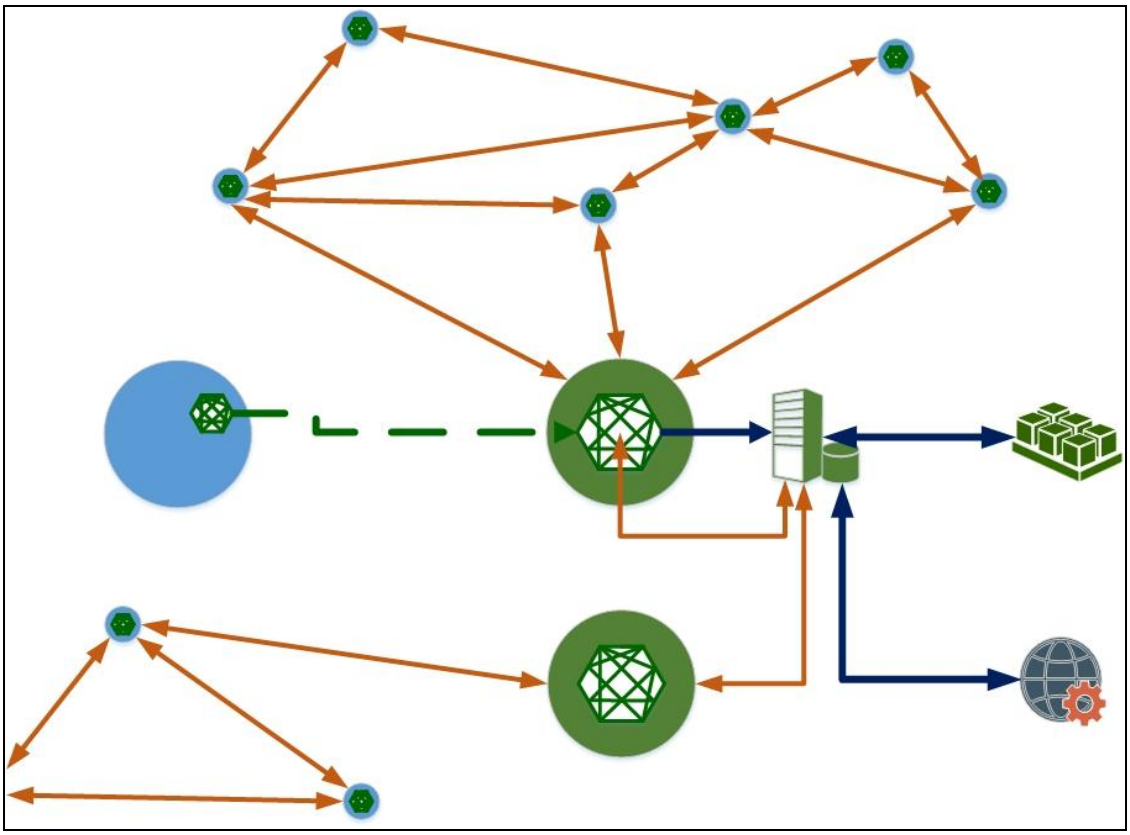
either the user device with installed client program, or other network nodes carrying functional features of the program responsible for notifications. The client program blocks the threat on all users notified via special program features, which scan for various sources of threats. The source of threat stands for any set of binary data in any form received by any communication channels or present on the user device.

BRIEF DESCRIPTION OF THE DRAWINGS

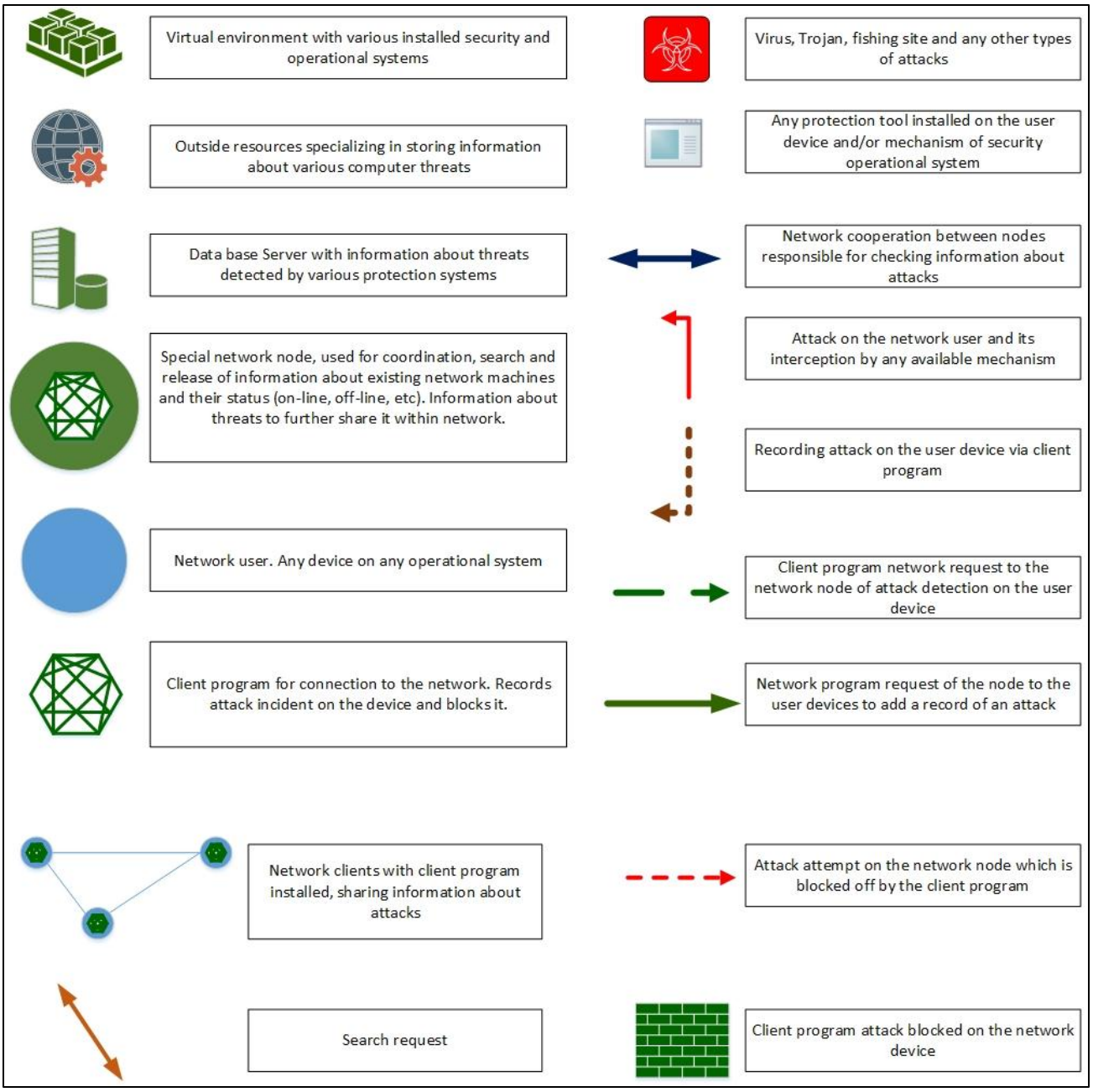
A clear understanding of the key features of the invention summarized above may be had by reference to the appended drawings, which illustrate the method and system of the invention, although it will be understood that such drawings depict preferred embodiments of the invention and, therefore, are not to be considered as limiting its scope with regard to other embodiments which the invention is capable of contemplating. Accordingly:



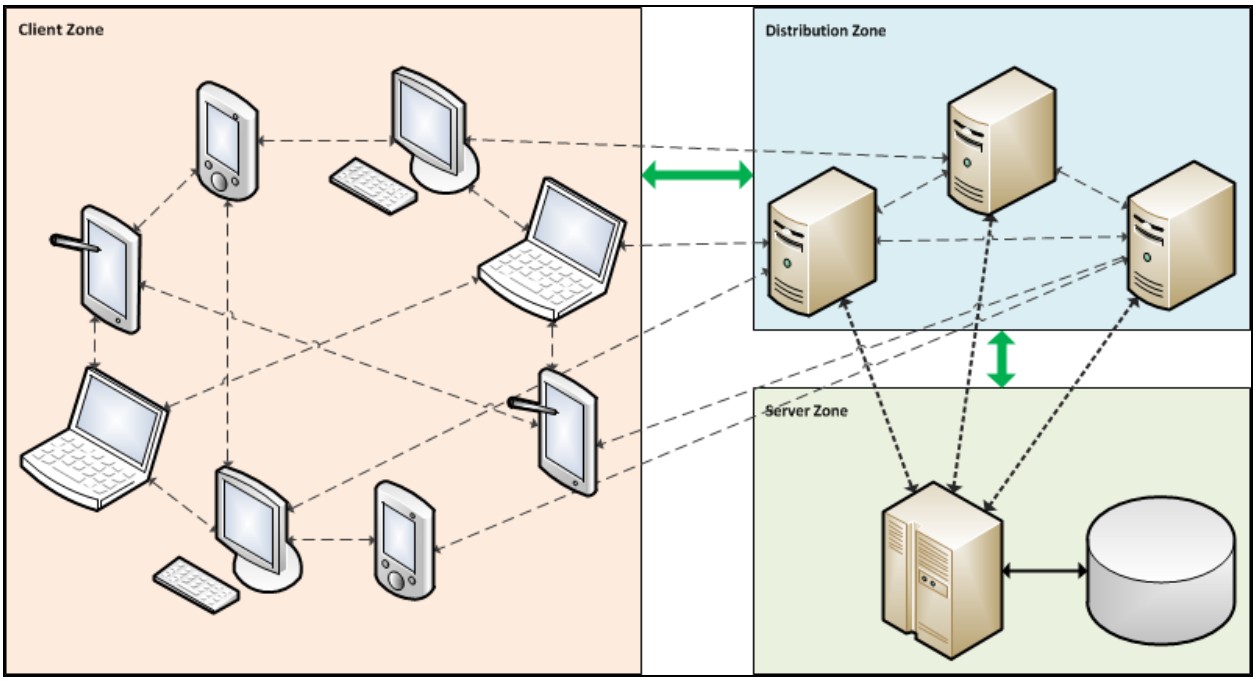
Drawing 1



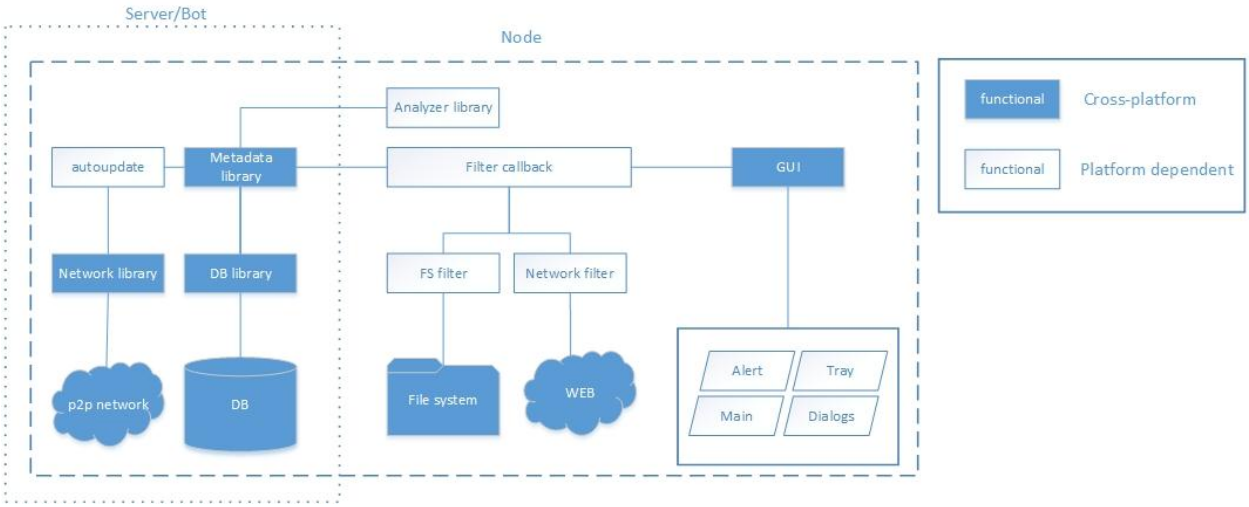
Drawing 2


Virtual environment with various installed security and operational systems
Virus, Trojan, fishing site and any other types of attacks
Outside resources specializing in storing information about various computer threats
Any protection tool installed on the user device and/or mechanism of security operational system
Data base Server with information about threats detected by various protection systems
Network cooperation between nodes responsible for checking information about attacks
Special network node, used for coordination, search and release of information about existing network machines and their status (on-line, off-line, etc). Information about threats to further share it within network.
Attack on the network user and its interception by any available mechanism
Recording attack on the user device via client program
Network user. Any device on any operational system
Client program network request to the network node of attack detection on the user device
Client program for connection to the network. Records attack incident on the device and blocks it.
Network program request of the node to the user devices to add a record of an attack
Network clients with client program installed, sharing information about attacks
Attack attempt on the network node which is blocked off by the client program
Search request
Client program attack blocked on the network device

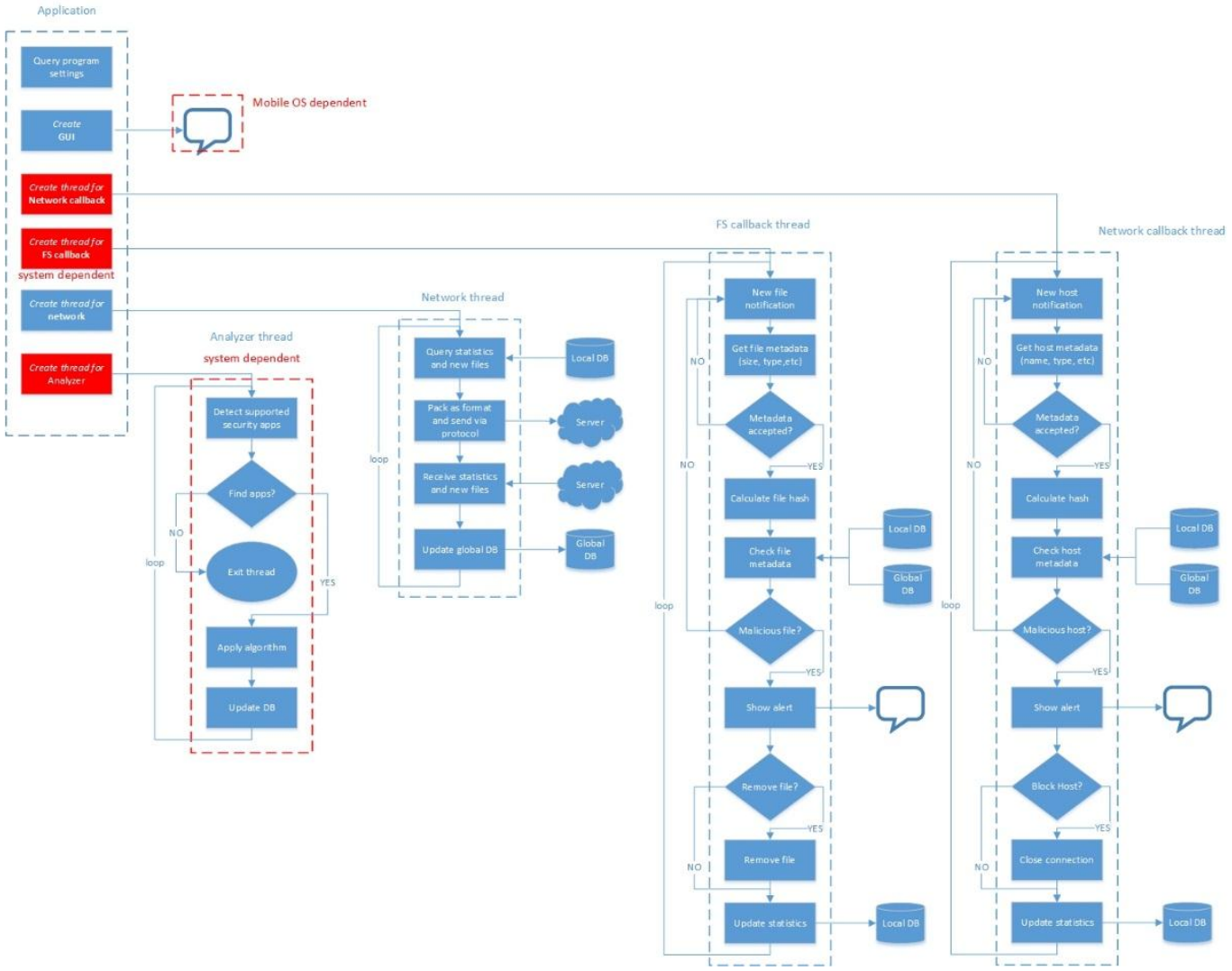
Drawing 3



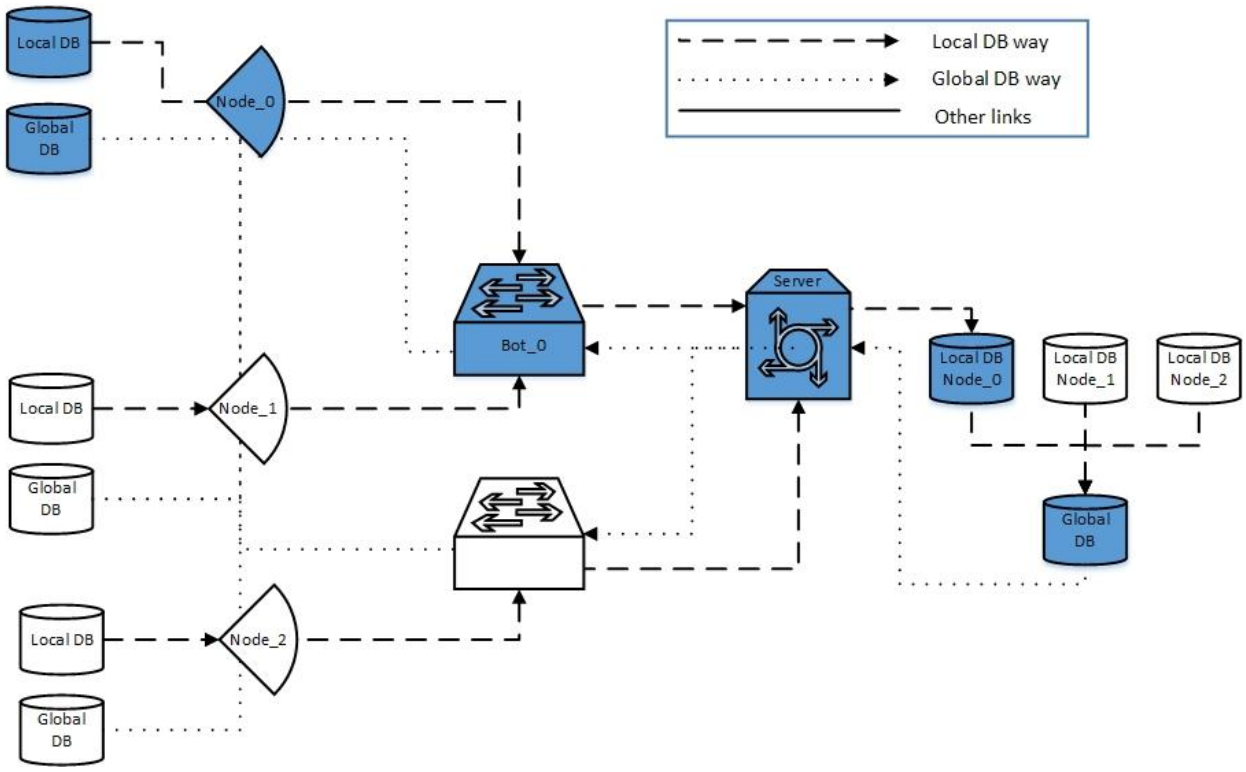
Drawing 4



Drawing 5


Application
Query program settings
Create GUI
Mobile OS dependent
Create thread for Network callback
Create thread for FS callback
system dependent
Create thread for network
Create thread for Analyzer
Analyzer thread
system dependent
Detect supported security apps
Find apps?
NO
loop
Exit thread
YES
Apply algorithm
Update DB
Network thread
Query statistics and new files
Local DB
Pack as format and send via protocol
Server
loop
Receive statistics and new files
Server
Update global DB
Global DB
FS callback thread
New file notification
NO
Get file metadata (size, type,etc)
Metadata accepted?
NO
YES
Calculate file hash
Check file metadata
Local DB
Global DB
loop
Malicious file?
YES
Show alert
Remove file?
YES
NO
Remove file
Update statistics
Local DB
Network callback thread
New host notification
NO
Get host metadata (name, type, etc)
Metadata accepted?
NO
YES
Calculate hash
Check host metadata
Local DB
Global DB
loop
Malicious host?
YES
Show alert
Block Host?
YES
NO
Close connection
Update statistics
Local DB

Drawing 6



Drawing 7

***DRAWING 1*.**

Illustrating mean and system of the invention. General simplified logic with the step be step algorithm.

***DRAWING 2*.**

Illustrating mean and system of the invention. Simplified logic of network operation in cases required for additional information search at network nods.

***DRAWING 3*.**

Illustrates main symbols utilized in Drawing 1 and 3.

***DRAWING 4*.**

Chart reflecting peer-to-peer network interface divided by zones

***DRAWING 5*.**

Chart reflecting a client program consisting of components and modules that are program functions

***DRAWING 6*.**

Reflecting work logic of the client-program for detection and prevention cyber threats as well as interconnection between system modules and components.

***DRAWING 7*.**

Reflecting client-program logic in local and remote database containing records regarding detected cyber threats.

DETAILED DESCRIPTION OF THE INVENTION

With the reference to *DRAWING 1 u DRAWING 3 step by step process is shown where* Step (1). A computer virus or any other kind of threat tries to attack a user with a client program installed. User protection systems blocks this attack. (Step 2). The application records this attack and the fact of it being blocked by the protection system. (Step 3). Then it sends a special request about this incident to any available node in the network. (Step 4). Having received this request, the node sends it to be checked for validity to the server with an installed database that contains information about threats. (Step 5). Furthermore, if this request returns no information about attack in the database, it runs another check via outside-specialized sources. (Step 6). If such check returns no result, then the checks continues in virtual environment through various installed protection tools. (Step 7). The result of such checks is then returned to the node(s). (Step 8). If it is positive and proves to be valid, then this information is shared with all users of the network. (Step 9). Network users then spread this information among all members of the network. (Step 10). In case of an attack attempt on any network user, the system blocks this threat in the user device, regardless of any installed protection system on the device or its ability to block such type of attack (Step 11).

In DRAWING 2 step-by-step process is shown if a check (Step 7) returned neither positive nor negative result, then a request is generated to search for the threat among other members of the network with a client program installed in order to confirm or refute the incident. In case of a positive result of the search, all network users are notified and the incident is recorded in the database of incidents.

DRAWING 4 reflects main components of informational security network. Network communication is built on a principle of peer-to-peer networks, broken into zones. Each zone has its own function

and visibility range in regards to other zones. Network architecture includes *CLIENT ZONE.* This zone is public, covered by the Internet and Intranet networks. This zone contains user devices regardless of operational system type. A node is any device from the client zone that has client program installed and covers the following functions:

- To establish connection with gateway, receive information about the nodes that hold actual information
- To establish connection with other nodes to download actual information
- To open ports and transfer requested information to other nodes.

Since nodes are in open availability, they are in the risk group and will be subject to analysis. To prevent interference in the network, nodes do not contain any information that can compromise server zone. Network architecture includes *DISTRIBUTION ZONE.* The main function of this zone is sharing information between the nodes. In addition, this zone is responsible for connecting the nodes to the server(s), excluding direct interaction of the latter. This zone is in the Internet network. Its elements are working stations, called gateways. Gateways are:

- To receive connections from the client zone nodes and transfer actual information about other nodes
- To establish connection with the server, receive and transfer actual information to the network nodes
- To open ports and transfer requested information to the nodes.

If the gateway is not responsive, a new one, without interference to the network, replaces it.

Network architecture includes SERVER ZONE this zone is a set of device and program software that covers the whole range of necessary functions (server, database, virtual environment, etc) to prove the validity of a detected threat, record statistics and analysis of the date in the network.

DRAWING 4 reflects application architecture. The application can be divided into 3 types according to its functions: Node, Bot and Server. More details about each of these types are provided under Network Architecture в depending on the zone of application location. Client Program (to be referred to as Application further on) consists of the components and nodes. Their list and functions are described below:

- Analyzer library – dynamic or static library combining nodes functions, collecting metadata and analyzing it. Collection of the metadata is done by the following methods:
    1. Parsing of the logged in incidents in security apps and other apps of the operational system.

2. Notification of a new incident the moment it happens by security systems via special API installed on the device.
3. Receipt of the list of system pings and API initiated by the security systems of the operational system and/or security apps.

Having received metadata via the methods described above, the component analyzes it based on the algorithm and determines the presence of a threat on a device. Described methods work in user mode and the core of the operational system mode. They can be installed in OS as systems service, drivers, etc. The final product of such a module is a conclusion whether the user device is subject to threat or not.

- Metadata library – dynamic or static library combining module functions, collecting metadata:
    1. Files hash, size, type, date started/modified/opened, harmful files, domains, and hosts.
    2. Creator and version of the installed security systems on the device.
    3. Systems functions pinged by security systems and their ping order.

- DB Library – dynamic or static library combining work functions with database.
- DB – database (relational and/or graph) which function is to store data in key-meaning pattern. This database contains information about harmful objects.
- Autoupdate – module responsible for updates and data synchronization.
- Network Library – module responsible for communication with hosts connected to the network via various protocols.
- Filter callback – module responsible for decision making on whether to notify user and block the file and/or host in regards to the user reply and file detection in the database.
- FS filter – file filter for monitoring new objects created and blocking them depending on the filter callback.
- Network filter – network filter for monitoring harmful objects appearance in network traffic and blocking it depending on the filter callback
- GUI – user application interface

DRAWING 6 reflects algorithm of application. The application is installed in the OS with necessary rights. By means of its own algorithms of processing collected metadata module, Metadata Library detects the moment of attack and/or threat. It then records this information in the local database. Then it synchronizes information from the local database with the global database. Then it shares this information via various communication protocols with members of this network.

It blocks the threat based on the records of local and global databases via mechanisms of callback functions installed on the file, network and other operations performed by the OS. Blocking threat

takes place if metadata from database of threats matched the metadata returned to the installed callback functions.

DRAWING 7 reflects network architecture of database. The application works with several databases: local and global. Local Database contains information about each recorded threat incident on this node by the Analyzer library module. It is then sent to the central server via bots. Global database - a unified database that contains information, collected from all nodes. It is a compilation of local databases of all nodes. It is configured on the server and spread between all nodes via bots and nodes themselves. Local database is used to add newly recorded attacks. It undergoes a preliminary check on the central server.

The present invention does not depend on what type of protection software is installed on their devices and if this software is able to handle this threat. Program efficiency and functionality is achieved by connecting devices (referred to as nodes further on) by our program into a unified one-tier network capable of fast communication exchange between nodes within the network about detected threats as reported by any of the users regardless of:

- Whether protection or antivirus software is installed on each node of this network or not
- Whether protection application is capable of sheltering the user from the threat or not
- Whether any protection software or application is installed on the user device or not.

While the present invention has been described in terms of particular embodiments and applications, in both summarized and detailed forms, it is not intended that these descriptions in any way limit its scope to any such embodiments and applications, and it will be understood that many substitutions, changes and variations in the described embodiments, applications and details of the method and system illustrated herein and of their operation can be made by those skilled in the art without departing from the spirit of this invention.

ABSTRACT

This invention provides improved protection from the computer viruses, malware and network security threats. The system and the mean include data exchange phases between devices about the threats detected in operating system.

System that allows regardless abilities of installed anti-virus/security software to prevent computer threats. The system and the mean that allows detecting and analyzing cyber attack attempt facts in operation system. The mean incudes the possibility to analyze and monitor computer systems behavior when detecting threats by other defensive devices.

CLAIMS

1. The method of provision of preventive defense of operation systems includes following stages:

Obtaining information about neutralized malware by different security systems at network nods;

Cyber threat Information verification

Notification of the network nods about security threat

Blocking and neutralization of the malware files and suspicions network resources at nods;

2. The method of claim 1, to analyze order to call up system functions in operating system by different security tools in relation to suspicious objects

3. The method of claim 1 to analyze event journals of operation system

4. The method of claim 1 to analyze even journals of security tools installed in operation system

5. The method of claim 1 to obtain metadata related to suspicious object from security tools and/or anti-virus software utilizing specialized API
6. The method of claim 1 to transmit data detected in claim 2, 3, 4 to network nods utilizing specially designed network requests
7. The method of claim 1 where data detected in claim 2,3,4 is verified in databases from different sources including nods data
8. The method of claim 1 to search data detected in claim 2,3,4 at the nodes connected to network
9. The method of claim 1 to segregate false and true data from the data detected in claim 2,3,4
10. The method of claim 1 to update registered threats database in real time manner
11. The method of claim 1 to neutralize and notify end-user about which security system detected the threat as a true one
12. The method of claim 1 to rank the registered threat based on end-user actions