**Ex. A-1 - Invalidity of U.S. Patent No. 8,543,710 against U.S. 9,398,037 to Roskind et al. ("Roskind")**

Fortinet, Inc. ("Fortinet") provides this chart subject to all reservations, objections, statements, and disclaimers set forth herein and in Fortinet's Preliminary Invalidity Contentions Cover Pleading, as well as any amendment, supplement, or modification thereof, which are incorporated herein by reference in their entirety.

On information and belief, and subject to further investigation and discovery, Roskind was filed September 27, 2005, and claims priority to Provisional application No. 60/613,909, filed on September 27, 2004, and is thus available as prior art under at least pre-AIA §102(e).

As illustrated in the chart below, Roskind anticipates the asserted claims of the '710 Patent. To the extent Roskind is found not to expressly disclose certain limitations in the asserted claims, such limitations are inherent. To the extent Roskind is found not to anticipate any asserted claims or claim elements of the '710 Patent, the reference nevertheless renders those claims or claim elements obvious under 35 U.S.C. § 103, either alone or in combination with other art identified in the cover pleading or herein. These Preliminary Invalidity Contentions are not an admission by Fortinet that the accused products, including any current or past versions of the accused products, are covered by, or infringe the asserted claims, but are based instead on the recognition that if the claims are interpreted to be broad enough to encompass the accused products, the claims must also be construed to have that same scope when considering whether they are invalid.

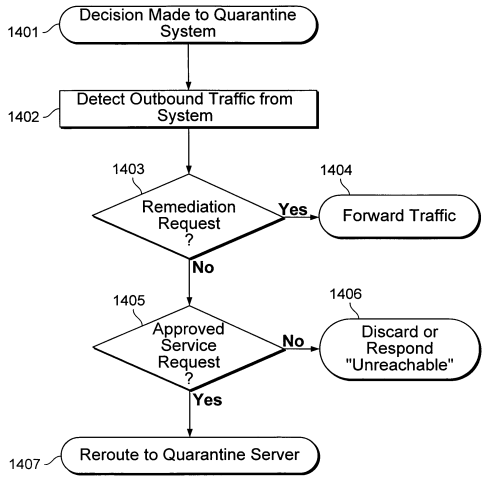
The following chart is partially based on, but is not limited by, the claim constructions implicit in Plaintiff's Infringement Contentions, to the extent that such constructions are apparent from the Infringement Contentions. Fortinet notes that in many instances, Plaintiff's Infringement Contentions fail to provide adequate notice of Plaintiff's construction of the asserted claims and fail to comply with the Court's scheduling order and other applicable rules. Fortinet does not accept the assumptions concerning the scope and meaning implicit in Plaintiff's Infringement Contentions, to the extent those assumptions are discernible, and reserves the right to challenge Plaintiff's proposed (or implied) constructions. Fortinet also reserves the right to revise and supplement these charts if and when Plaintiff is permitted to provide revised Infringement Contentions or otherwise make its positions known. To the extent that these Preliminary Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the asserted claims, Fortinet does not necessarily advocate any such construction as proper constructions of those terms or phrase. Fortinet also reserves the right to revise and supplement these charts after the Court construes the claims. Citations given in the chart below are merely representative of the respective elements and are not meant to be exhaustive.

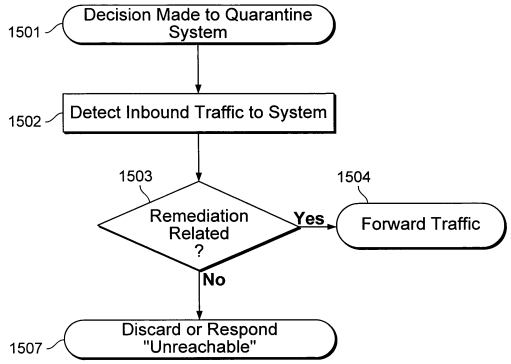


Netskope, Ex. 2003
Fortinet v. Netskope, IPR2026-00042

| Claim | Exemplary Citation from Roskind |
|---|---|
| **[1pre]** A method of network traffic quarantine control, comprising: | Roskind discloses and/or renders obvious a method of network traffic quarantine control.<br><br>*E.g.*:<br><br>Roskind at 1:14-43:<br>"Unwanted and/or malicious network communications, such as spam, phishing, worm propagation, etc., hamper productivity and the use and enjoyment of computer and network resources by end users, burden affected networks with unauthorized and/or undesired traffic, and expose recipients to the risk of theft, fraud, etc. Current technologies for dealing with such unauthorized and/or unwanted communications focus on filtering messages at a point in the communication path close to the recipient system, such as anti-spam and/or other security software installed on the destination host and/or a local mail (or other messaging) server to which communications, to the destination host are directed for delivery to the destination host, e.g., by detecting messages sent by blacklisted senders and/or messages containing header or other content that indicates the message is suspicious. While this approach can be an effective way to protect an individual host or a group of destination hosts served by a local server, it does not address the network congestion problem and leaves vulnerable hosts not protected by destination (or destination mail or messaging server) based filtering software. In addition, in many cases an attacker causes each of one or more compromised hosts to send multiple instances of a malicious communication, often simultaneously or nearly so, magnifying the effect on the network. Therefore, there is a need for an effective way to intercept and take corrective action with respect to unauthorized, unwanted, and/or otherwise malicious electronic mail and/or other network communications that better protects the network and provides protection to destination hosts that are not protected by destination or destination mail or messaging server based filtering software."<br><br>Roskind at 11:15-56:<br><br>"FIG. 10A is a flow diagram of a method for identifying and remedying problems according to some embodiments. A problem may be identified as some event or status that may cause direct or potential harm. Exemplary problems include vulnerability or infestation. In this example, a problem such as a vulnerability or infestation is detected (1001). Infestation herein refers to the current presence and/or execution of contagion. In some embodiments, detection may be made by a router, firewall, or other |

| Claim | Exemplary Citation from Roskind |
| --- | --- |
| | network component, separately or in concert, using techniques such as those illustrated by FIGS. 11, 12, and 13. In some embodiments, detection may be made by a computing device, for example a computing device operated by an ISP. After a detection of a problem, a computer or network containing the problem is quarantined (1002). In some embodiments, quarantining includes preventing unauthorized communications from being sent from the quarantined computer, such as efforts to infect, probe, or harass other computers, or efforts to communicate data without authorization, including for example file contents and keyboard entry logs. In some embodiments, no communications are authorized. In some embodiments, quarantining includes preventing undesired communications from reaching the quarantined computer, such as control messages or infectious messages. Examples of quarantining activities are illustrated in FIGS. 14 and 15. In this example, the quarantined computer is provided access to remediation services (1003). In some embodiments, access to remediation includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor's server, or providing virus and worm disinfecting tools, such as focused removal tools, or data updates for previously installed repair tools. In some embodiments, access to remediation includes allowing direct access to vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained. In some embodiments, access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443, certain content requests, such as specific URLs or specific file downloads. In some embodiments, remediation content may be substituted for other requested content, for example as discussed in conjunction with FIG. 14." |

| Claim | Exemplary Citation from Roskind |
| --- | --- |
| | Figure 14   FIG. 14 |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Figure 15<br><br><br>FIG. 15 |
| **[1a]** at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network; | Roskind discloses and/or renders obvious at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network.<br><br>*E.g.*:<br><br>Roskind at 11:57-12:13:<br>"FIG. 10B is a block diagram illustrating a network environment in which infected hosts and/or networks are quarantined according to some embodiments. A plurality of hosts 1 to "m", represented in FIG. 10B by hosts 1020, 1022, and 1024, connect via a router 1026 and a gateway 1028 to the Internet 1030. In various embodiments the router 1026 is omitted or included in the gateway 1028. In various embodiments, gateway 1028 comprises a gateway, router, firewall, or other device configured to provide and control access between a protected network and the Internet and/or another public or private network. In various embodiments, the pro cess of FIG. 10A is implemented, in the event of quarantine of one or more of hosts 1020-1024, for example, on the affected (quarantined) host, router 1026, and/or gateway 1028. In some embodiments, a quarantined host (or a host associated with a quarantined network or sub-network) is permitted to access a remediation server |

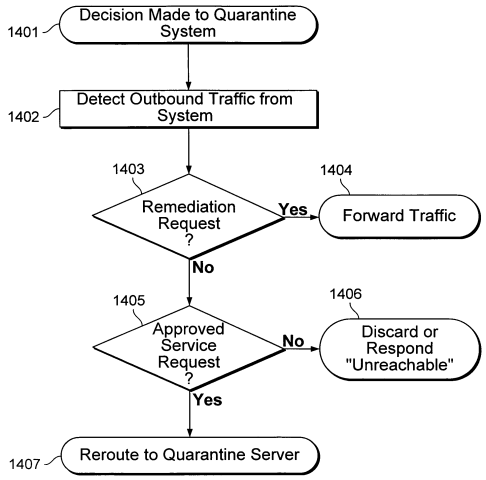
| Claim | Exemplary Citation from Roskind |
|---|---|
| | 1032, e.g., to download a patch, more current threat definition, etc. In some embodiments, requests to connection to a host other than the remediation server 1032 are redirected to a quarantine server 1034 configured to provide a notice and/or other information and/or instructions to a user of the quarantined host. In various alternative embodiments the quarantine server 1034 is omitted or resides on the router 1026 and/or gateway 1028."<br><br>Roskind at 14:27-15:12:<br>"FIG. 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with FIG. 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. In some embodiments, requests for a quarantine may be made on an individual computer via settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic. is tested in this example to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in |

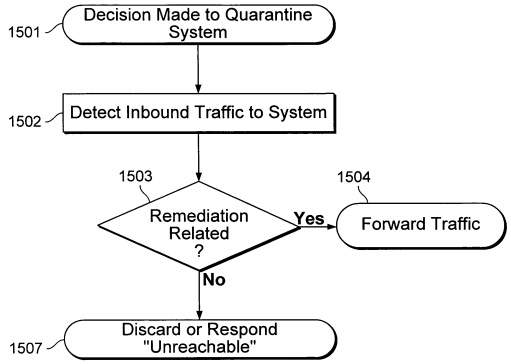
| Claim | Exemplary Citation from Roskind |
|---|---|
| | remediation. Rerouting of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of rerouting a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example."<br><br>Roskind at 16:44-17:45:<br>"FIG. 17 is a flow diagram of a method for scanning backdoors and inoculating according to some embodiments. In this example, preparations are made for scanning a computer for a backdoor inoculation path (1701), for example by identifying the computer to be scanned, and enumerating or retrieving a list of one or more backdoors. In one example, an IP address to be scanned may be selected by an ISP from a list of subscribers. In one example, a list of backdoors may include information associated with preloaded software approved by the computer owner for access and inoculation purposes, such as an ISP provided utility that is installed by the subscriber. In some embodiments, an ISP defined backdoor may have an authentication protocol to preclude control by unauthorized parties, such as restrictions on IP address(es) that may contact the backdoor, or shared secrets such as a password required by the sender, or cryptographic authentication such as client authentication on an SSL connection. In some embodiments, a user is requested and/or required to authorize in advance use of an authorized and/or any unauthorized backdoor for purposes of inoculation. As another example, a list of backdoors may include virus or worm installed backdoors, such as those installed by a SubSeven virus or Back Orifice. As another example, backdoors may include exploitable security vulnerabilities, such as a weak  ness in a web server, or a weakness in an RPC service. A scan may optionally be conducted to detect open TCP/IP backdoor ports (1702) similarly to the scan discussed in conjunction with FIG. 11. If none of the backdoors are open (1703), for example there is no response on any of the ports, then the scan is complete (1706) in this example. If one or more backdoor ports are open (1703) then they are tested for usability (1704) in this example. In some embodiments, a backdoor port may be assumed open (1703) and may be tested for usability (1704) without an independent test to see if the port is open. An example of a usability test is no test at all, with the conclusion that a specific port is usable any time it is open. Another example of a usability test is based on the receipt of confirmation of a functional installation of ISP |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | provided backdoor software, such as a confirmation that may be provided by the installed software. Another example of a usability test involves the use of a less invasive test of vulnerabilities such a buffer overrun exploit that does not have a permanent impact but provides observable validation (such as a dropped connection). If a backdoor is usable (1705) then the computer is inoculated via a backdoor (1707) in this example. One example of such an inoculation is the remotely controlled download of one or more remedy files into one or more directories, such as an operating system directory, such as the "\windows\system" directory in Microsoft Windows 2000. Another example of an inoculation is the download of an executable file to the computer, followed by the execution of that file. Another example of an inoculation is the download of a data file, such as an anti-contagion signature file, that is interpreted or processed by another executable already on the computer. Another example of an inoculation is the deletion of one or more files from the computer. Another example of an inoculation is the editing of one or more registry entries, or of one or more files, such as deleting, appending or rewriting entries in a registry or file. Another example of inoculation includes a combination of one or more of above techniques, optionally in conjunction with one or more remotely instigated reboot operations. Another example of inoculation includes a combination of one or more of the above techniques, along with an optional dialog box requesting a user's permission to proceed with the inoculation. Another example of inoculation is the use of a dialog box in conjunction with a timer that causes the inoculation to proceed if no user response is given in a prescribed period of time, such as 1 hour." |
| **[1b]** at the network access gateway device, performing a plurality of quarantine control functions over the client device, wherein the plurality of quarantine control functions comprises: | Roskind discloses and/or renders obvious at the network access gateway device, performing a plurality of quarantine control functions over the client device.<br><br>*E.g.*,:<br><br>Roskind at 11:15-56:<br>"FIG. 10A is a flow diagram of a method for identifying and remedying problems according to some embodiments. A problem may be identified as some event or status that may cause direct or potential harm. Exemplary problems include vulnerability or infestation. In this example, a problem such as a vulnerability or infestation is detected (1001). Infestation herein refers to the current presence and/or execution of contagion. In some embodiments, detection may be made by a router, firewall, or other network component, separately or in concert, using techniques such as those illustrated by FIGS. 11, |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | 12, and 13. In some embodiments, detection may be made by a computing device, for example a computing device operated by an ISP. After a detection of a problem, a computer or network containing the problem is quarantined (1002). In some embodiments, quarantining includes preventing unauthorized communications from being sent from the quarantined computer, such as efforts to infect, probe, or harass other computers, or efforts to communicate data without authorization, including for example file contents and keyboard entry logs. In some embodiments, no communications are authorized. In some embodiments, quarantining includes preventing undesired communications from reaching the quarantined computer, such as control messages or infectious messages. Examples of quarantining activities are illustrated in FIGS. 14 and 15. In this example, the quarantined computer is provided access to remediation services (1003). In some embodiments, access to remediation includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor's server, or providing virus and worm disinfecting tools, such as focused removal tools, or data updates for previously installed repair tools. In some embodiments, access to remediation includes allowing direct access to vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained. In some embodiments, access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443, certain content requests, such as specific URLs or specific file downloads. In some embodiments, remediation content may be substituted for other requested content, for example as discussed in conjunction with FIG. 14."<br><br>Roskind at 14:27-15:12:<br>"FIG. 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with FIG. 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. |

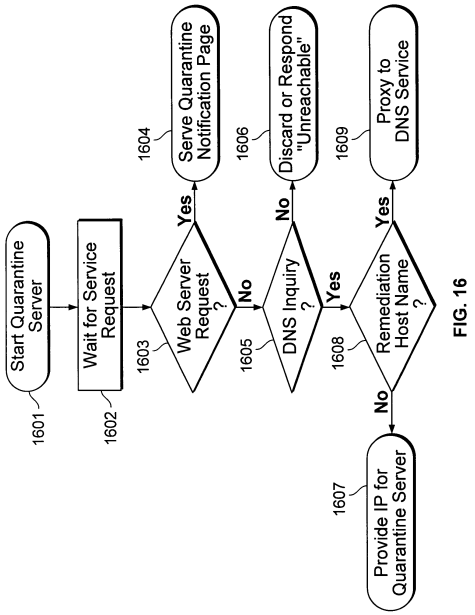
| Claim | Exemplary Citation from Roskind |
|---|---|
| | In some embodiments, requests for a quarantine may be made on an individual computer via settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic. is tested in this example to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation. Rerouting of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of rerouting a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example." |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Figure 14   FIG. 14 |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Figure 15<br><br><br>FIG. 15 |
| **[1b(a)]** restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment; | Roskind discloses and/or renders obvious restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment.<br><br>*E.g.*,:<br><br>Roskind at 11:15-56:<br>"FIG. 10A is a flow diagram of a method for identifying and remedying problems according to some embodiments. A problem may be identified as some event or status that may cause direct or potential harm. Exemplary problems include vulnerability or infestation. In this example, a problem such as a vulnerability or infestation is detected (1001). Infestation herein refers to the current presence and/or execution of contagion. In some embodiments, detection may be made by a router, firewall, or other network component, separately or in concert, using techniques such as those illustrated by FIGS. 11, 12, and 13. In some embodiments, detection may be made by a computing device, for example a computing device operated by an ISP. After a detection of a problem, a computer or network |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | containing the problem is quarantined (1002). In some embodiments, quarantining includes preventing unauthorized communications from being sent from the quarantined computer, such as efforts to infect, probe, or harass other computers, or efforts to communicate data without authorization, including for example file contents and keyboard entry logs. In some embodiments, no communications are authorized. In some embodiments, quarantining includes preventing undesired communications from reaching the quarantined computer, such as control messages or infectious messages. Examples of quarantining activities are illustrated in FIGS. 14 and 15. In this example, the quarantined computer is provided access to remediation services (1003). In some embodiments, access to remediation includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor's server, or providing virus and worm disinfecting tools, such as focused removal tools, or data updates for previously installed repair tools. In some embodiments, access to remediation includes allowing direct access to vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained. In some embodiments, access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443, certain content requests, such as specific URLs or specific file downloads. In some embodiments, remediation content may be substituted for other requested content, for example as discussed in conjunction with FIG. 14."<br><br>Roskind at 14:27-15:12:<br>"FIG. 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with FIG. 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. In some embodiments, requests for a quarantine may be made on an individual computer via settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for |

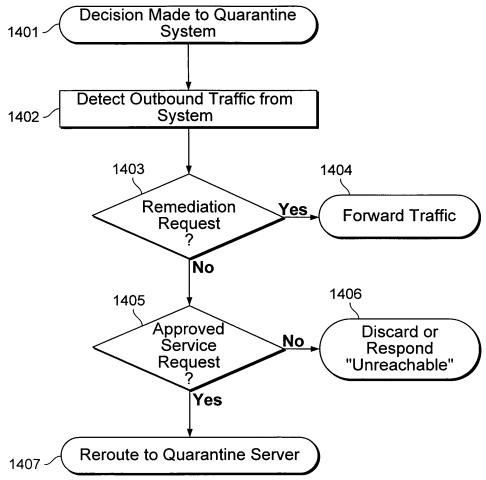
| Claim | Exemplary Citation from Roskind |
|---|---|
| | example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic. is tested in this example to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation. Rerouting of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of rerouting a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example."<br><br>Roskind at 15:36-56:<br>"In some embodiments, a configuration based quarantine during an installation of an operating system, such as Microsoft Windows, may be automatically setup, for example by a default installation setting up restrictions in a firewall installed with the OS or by an installation setting defaults for use when network connectivity is enabled, that establishes a quarantine, for example restricting internet connections, for example allowing internet connections only to a security. update site such as Microsoft Windows Update. In some embodiments, settings that may establish a quarantine, such as default settings in an operating system installation, may be altered programmatically to remove the quarantine in response to a remediation site, such as a security update service such as Microsoft Windows Update, asserting that there are no other security updates pending. In some embodiments, configuration settings that may establish a quarantine may be altered |

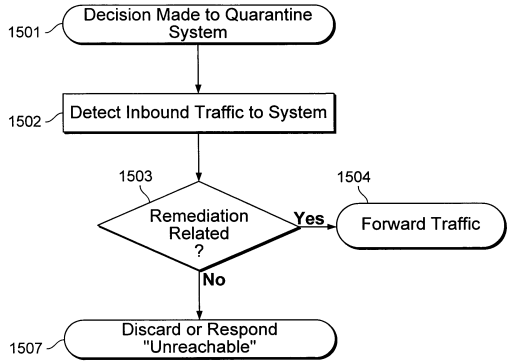
| Claim | Exemplary Citation from Roskind |
|---|---|
| | programmatically to enable a quarantine in response to the presence of one or more security updates, such as provided by an operating system update service such as Microsoft Windows Update, that are available for installation on a computer."<br><br>Figure 16<br><br><br>FIG. 16 |
| **[1b(b)]** restricting all network traffic emanating from the client device to an allowed network destination address to selected one or | Roskind discloses and/or renders obvious restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols.<br><br>*E.g.*: |

| Claim | Exemplary Citation from Roskind |
|---|---|
| more network protocols; and | Roskind at 11:15-56:<br>"FIG. 10A is a flow diagram of a method for identifying and remedying problems according to some embodiments. A problem may be identified as some event or status that may cause direct or potential harm. Exemplary problems include vulnerability or infestation. In this example, a problem such as a vulnerability or infestation is detected (1001). Infestation herein refers to the current presence and/or execution of contagion. In some embodiments, detection may be made by a router, firewall, or other network component, separately or in concert, using techniques such as those illustrated by FIGS. 11, 12, and 13. In some embodiments, detection may be made by a computing device, for example a computing device operated by an ISP. After a detection of a problem, a computer or network containing the problem is quarantined (1002). In some embodiments, quarantining includes preventing unauthorized communications from being sent from the quarantined computer, such as efforts to infect, probe, or harass other computers, or efforts to communicate data without authorization, including for example file contents and keyboard entry logs. In some embodiments, no communications are authorized. In some embodiments, quarantining includes preventing undesired communications from reaching the quarantined computer, such as control messages or infectious messages. Examples of quarantining activities are illustrated in FIGS. 14 and 15. In this example, the quarantined computer is provided access to remediation services (1003). In some embodiments, access to remediation includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor's server, or providing virus and worm disinfecting tools, such as focused removal tools, or data updates for previously installed repair tools. In some embodiments, access to remediation includes allowing direct access to vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained. In some embodiments, access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443, certain content requests, such as specific URLs or specific file downloads. In some embodiments, remediation content may be substituted for other requested content, for example as discussed in conjunction with FIG. 14."<br><br>Roskind at 14:27-15:12:<br>"FIG. 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with FIG. 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. In some embodiments, requests for a quarantine may be made on an individual computer via settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic. is tested in this example to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation. Rerouting of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of rerouting a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example." |

| Claim | Exemplary Citation from Roskind |
| --- | --- |
| | Roskind at 15:36-56:<br>"In some embodiments, a configuration based quarantine during an installation of an operating system, such as Microsoft Windows, may be automatically setup, for example by a default installation setting up restrictions in a firewall installed with the OS or by an installation setting defaults for use when network connectivity is enabled, that establishes a quarantine, for example restricting internet connections, for example allowing internet connections only to a security. update site such as Microsoft Windows Update. In some embodiments, settings that may establish a quarantine, such as default settings in an operating system installation, may be altered programmatically to remove the quarantine in response to a remediation site, such as a security update service such as Microsoft Windows Update, asserting that there are no other security updates pending. In some embodiments, configuration settings that may establish a quarantine may be altered programmatically to enable a quarantine in response to the presence of one or more security updates, such as provided by an operating system update service such as Microsoft Windows Update, that are available for installation on a computer." |

| Claim | Exemplary Citation from Roskind |
| --- | --- |
| | Figure 14   FIG. 14 |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Figure 15<br><br><br>FIG. 15 |
| **[1c]** rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device. | Roskind discloses and/or renders obvious rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device.<br><br>*E.g.*:<br><br>Roskind at 6:63-7:23:<br>"FIG. 4B is a block diagram of a client system configured to obtain an update according to some embodiments. In some embodiments, the client system shown in FIG. 4B is used to implement one or more of clients 220-224 of FIG. 2B. The client system 420 includes a communication interface 422, such as a network interface card, configured to send/receive communications via a network, such as the Internet. The client system 420 further includes an update agent and/or browser 424. In some embodiments, the update agent/ browser 424 comprises browser software used to navigate the World Wide Web, e.g., to send/receive data to/from a website from which an update is available for download. In some embodiments, update agent/browser 424 includes an agent associated with anti-contagion software installed on the client system 420. In various embodiments, the update agent/ |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | browser 424 comprises one or more components and is implemented as one or more software programs running on a processor and/or one or more hardware components. A settings data store 426 stores one or more settings and/or other data associated with the software with which an update and/or software to which the update does or may pertain, such as periodicity or next scheduled (e.g., reservation) time to check for updates, a list of update identifiers, locators, and/or redistribution sources from which an update is or may be available, policies for whether and/or under what terms, conditions, circumstances, etc. the client system 420 may be used redistribute an update, a last update time, an old version identifier (see, e.g., 202 of FIG. 2A), etc."<br><br>Roskind at 11:57-12:13:<br>"FIG. 10B is a block diagram illustrating a network environment in which infected hosts and/or networks are quarantined according to some embodiments. A plurality of hosts 1 to "m", represented in FIG. 10B by hosts 1020, 1022, and 1024, connect via a router 1026 and a gateway 1028 to the Internet 1030. In various embodiments the router 1026 is omitted or included in the gateway 1028. In various embodiments, gateway 1028 comprises a gateway, router, firewall, or other device configured to provide and control access between a protected network and the Internet and/or another public or private network. In various embodiments, the process of FIG. 10A is implemented, in the event of quarantine of one or more of hosts 1020-1024, for example, on the affected (quarantined) host, router 1026, and/or gateway 1028. In some embodiments, a quarantined host (or a host associated with a quarantined network or sub-network) is permitted to access a remediation server 1032, e.g., to download a patch, more current threat definition, etc. In some embodiments, requests to connection to a host other than the remediation server 1032 are redirected to a quarantine server 1034 configured to provide a notice and/or other information and/or instructions to a user of the quarantined host. In various alternative embodiments the quarantine server 1034 is omitted or resides on the router 1026 and/or gateway 1028."<br><br>Roskind at 15:57-16:43:<br>"FIG. 16 is a flow diagram of a method for a quarantine server to respond to requests according to some embodiments. In this example, a quarantine server is started (1601), for example by starting a web server, or DNS server, or proxy server, or ftp server, or some combination server. The server waits for a request (1602), for example by listening on a port and waiting for a connection. In some embodiments, a device such as a router may forward outbound traffic from a quarantined computer to |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | a quarantine server, for example as illustrated in conjunction with 1407 of FIG. 14. If a received connection is a web server request (1603), such as an HTTP request, then the server responds with a quarantine notification page (1604) in this example. An example of a quarantine notification page is a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain. The links on the quarantine notification page may be examples of HTTP addresses that are for use in remediation. Another example of a quarantine notification page is a page that redirects to a quarantine notification page. If the request is not a web server request (1603), then it is tested to see if it is a DNS inquiry (1605) in this example. A DNS inquiry may for example appear on port 53 using TCP/IP or UDP. If the request is not a DNS inquiry (1605) then it may be discarded or responded to as "unreachable" (1606) in this example. If the request is a DNS inquiry (1605) then, in this example, the inquiry is tested to see if it is a DNS request for a remediation host name (1608). A remediation host name may include a host name as appropriate to the reason for a quarantine, such as a host providing anti-contagion software, or a host providing security updates, or a host internal to (or partnered with) an ISP. If the DNS inquiry was for a remediation host name (1608) then the request is proxied to an external DNS service provider (1609) in this example. A proxy to a DNS service (1609) may return a stored or cached response, such as the actual IP address of the host name, or it may contact an external DNS service to relay back the proposed IP address. If the DNS inquiry was not for a remediation host name (1608) then an IP address for a quarantine server is provided (1607) in this example. In some embodiments, when a redirected IP address is provided, such as that of a quarantine server, the DNS response may include a short time to live, for example 0 seconds. A short time to live ensures that a further DNS query will be sent prior to subsequent communications being sent from the quarantined computer to the host that was the subject of the DNS query, aiding a return to normal routing of traffic once the computer is no longer under quarantine. In some embodiments, the server(s) in this example may continue to wait for a service request (1602) in parallel with the processing of the requests as described above, or may wait for a service request again after disposition of the previous request as described above." |
| **[2]** The method according to claim 1, wherein the action requires the user to obtain and execute abnormal | Roskind discloses and/or renders obvious the method according to claim 1, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses. |

| Claim | Exemplary Citation from Roskind |
|---|---|
| behavior scanning software from a server machine running at one of the one or more allowed network destination addresses. | *E.g.*:<br><br>Roskind at 5:66-6:62:<br>"FIG. 4A is a flow diagram of a method for acquiring an update according to some embodiments. In this example, an update source is contacted (401), such as via an Internet connection, for example via TCP/IP. An offer to serve as a redistribution source is made (402). In some embodiments, a redistribution source may be contacted by other computers to acquire an update. An example of an offer to be a redistribution server is described in conjunction with FIG. 6. In various embodiments, 402 is optional, performed only if a criterion or test is satisfied, or omitted. An update or an update identifier is acquired (403). An example of an update identifier is a version number for an update. Another example of an update identifier is a checksum for an update. Another example of an update identifier is a set of checksums (such as MD5, SHA-1, or CRC-32) for a corresponding set of byte ranges that form the update. Another example of an update identifier is a combination two or more identifiers, such as the identifiers enumerated above. If the update was completed (404) then the user confirms redistribution sourcing status (408) in this example. In some embodiments, confirmation includes asserting that the client is prepared to redistribute copies of the received data to one or more recipients. If the update was not completed (404), then a list of peer or other sources is acquired (405) in this example. In some embodiments, the list. is or may be explicit. In some embodiments, the list is or may be implicit, for example represented by an iterator or accessor, which may retrieve elements on an as needed basis. In some embodiments, implicit lists are dynamic, and calculated or created in part on an as needed or as requested basis. In some embodiments, the list of other sources contain addresses that may be contacted to acquire an update, such as a list of IP addresses and ports, as well as optionally some authentication information to be used when contacting a listed source. In some embodiments, a requesting host that agrees to serve as a redistribution source is provided with a list of sources from which the update is available immediately, or at least sooner than it will be made available to hosts that will not redistribute. One or more attempts may be made to acquire the update from a listed source (406), for example as exemplified in FIG. 8. If the update is completed via a listed source (407), then redistribution status is confirmed (408) in this example. If the update is not complete (407) then a reservation is optionally negotiated and/or acquired (409) in this example. In some embodiments, a reservation may include a time and/or a specific source or IP address. In some embodiments, a reservation address may be selected from a collection of source addresses, for example in order to distribute the load across more than one server, or to provide a server that is |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | closer to a recipient. An example of selecting a server close to a recipient is to select a server having relatively lower latency during a download, or relatively lower cost, for example by selecting a source within a recipient's ISP complex or within a recipient's intranet or home network. If a reservation time was acquired, then a wait for that reservation time (410) is performed in this example. At the reservation time, a further attempt to acquire an update or update identifier from the source (403) is made, and the flow proceeds as described earlier. This flow may continue until an acquisition is complete (408), as also described earlier. In various embodiments, one or more of confirming redistribution sourcing status (408), attempting to obtain the update from a redistribution source (405-407), and/or acquiring and/or waiting for a reservation time (409-410) is/are optional, conditional, or omitted."<br><br>Roskind at 6:63-7:23:<br>"FIG. 4B is a block diagram of a client system configured to obtain an update according to some embodiments. In some embodiments, the client system shown in FIG. 4B is used to implement one or more of clients 220-224 of FIG. 2B. The client system 420 includes a communication interface 422, such as a network interface card, configured to send/receive communications via a network, such as the Internet. The client system 420 further includes an update agent and/or browser 424. In some embodiments, the update agent/ browser 424 comprises browser software used to navigate the World Wide Web, e.g., to send/receive data to/from a website from which an update is available for download. In some embodiments, update agent/browser 424 includes an agent associated with anti-contagion software installed on the client system 420. In various embodiments, the update agent/ browser 424 comprises one or more components and is implemented as one or more software programs running on a processor and/or one or more hardware components. A settings data store 426 stores one or more settings and/or other data associated with the software with which an update and/or software to which the update does or may pertain, such as periodicity or next scheduled (e.g., reservation) time to check for updates, a list of update identifiers, locators, and/or redistribution sources from which an update is or may be available, policies for whether and/or under what terms, conditions, circumstances, etc. the client system 420 may be used redistribute an update, a last update time, an old version identifier (see, e.g., 202 of FIG. 2A), etc."<br><br>Roskind at 16:44-17:45: |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | "FIG. 17 is a flow diagram of a method for scanning backdoors and inoculating according to some embodiments. In this example, preparations are made for scanning a computer for a backdoor inoculation path (1701), for example by identifying the computer to be scanned, and enumerating or retrieving a list of one or more backdoors. In one example, an IP address to be scanned may be selected by an ISP from a list of subscribers. In one example, a list of backdoors may include information associated with preloaded software approved by the computer owner for access and inoculation purposes, such as an ISP provided utility that is installed by the subscriber. In some embodiments, an ISP defined backdoor may have an authentication protocol to preclude control by unauthorized parties, such as restrictions on IP address(es) that may contact the backdoor, or shared secrets such as a password required by the sender, or cryptographic authentication such as client authentication on an SSL connection. In some embodiments, a user is requested and/or required to authorize in advance use of an authorized and/or any unauthorized backdoor for purposes of inoculation. As another example, a list of backdoors may include virus or worm installed backdoors, such as those installed by a SubSeven virus or Back Orifice. As another example, backdoors may include exploitable security vulnerabilities, such as a weak  ness in a web server, or a weakness in an RPC service. A scan may optionally be conducted to detect open TCP/IP backdoor ports (1702) similarly to the scan discussed in conjunction with FIG. 11. If none of the backdoors are open (1703), for example there is no response on any of the ports, then the scan is complete (1706) in this example. If one or more backdoor ports are open (1703) then they are tested for usability (1704) in this example. In some embodiments, a backdoor port may be assumed open (1703) and may be tested for usability (1704) without an independent test to see if the port is open. An example of a usability test is no test at all, with the conclusion that a specific port is usable any time it is open. Another example of a usability test is based on the receipt of confirmation of a functional installation of ISP provided backdoor software, such as a confirmation that may be provided by the installed software. Another example of a usability test involves the use of a less invasive test of vulnerabilities such a buffer overrun exploit that does not have a permanent impact but provides observable validation (such as a dropped connection). If a backdoor is usable (1705) then the computer is inoculated via a backdoor (1707) in this example. One example of such an inoculation is the remotely controlled download of one or more remedy files into one or more directories, such as an operating system directory, such as the "\windows\system" directory in Microsoft Windows 2000. Another example of an inoculation is the download of an executable file to the computer, followed by the execution of that file. Another example of an inoculation is the download of a data file, such as an anti-contagion |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | signature file, that is interpreted or processed by another executable already on the computer. Another example of an inoculation is the deletion of one or more files from the computer. Another example of an inoculation is the editing of one or more registry entries, or of one or more files, such as deleting, appending or rewriting entries in a registry or file. Another example of inoculation includes a combination of one or more of above techniques, optionally in conjunction with one or more remotely instigated reboot operations. Another example of inoculation includes a combination of one or more of the above techniques, along with an optional dialog box requesting a user's permission to proceed with the inoculation. Another example of inoculation is the use of a dialog box in conjunction with a timer that causes the inoculation to proceed if no user response is given in a prescribed period of time, such as 1 hour." |
| **[6]** The method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment. | Roskind discloses and/or renders obvious the method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment.<br><br>*E.g.*:<br><br>Roskind at 13:10-53:<br>"FIG. 12 is a flow diagram of a method for identifying an infestation according to some embodiments. In this example, a device near a computer, such as a firewall on a LAN or an ISP's router, is used in some embodiments to monitor a computer for infestation (1201). Network traffic is monitored for anomalous traffic volume, port, or IP destination (1202), for example by detecting large volumes of outbound traffic, such as email traffic or instant messaging traffic. Another example of anomalous traffic is a TCP/IP connection to a server that is known to control a collection of infested machines, in a way that suggests the connecting machine is controlled by the server, such as connecting and transmitting an assertion that it is controlled or available to comply. Another example of anomalous traffic is a connection to a computer that is a current target of a denial of service attack, with a pattern that is consistent with the attack, such as a connection to a targeted port, or the use of a falsified return IP address. In some embodiments, a falsified return address may be detected by a router, such as an ISP router, that is aware that the return address is not on the sourcing subnet, or not associated with the MAC address that has supplied the corresponding packets. If an anomaly is |

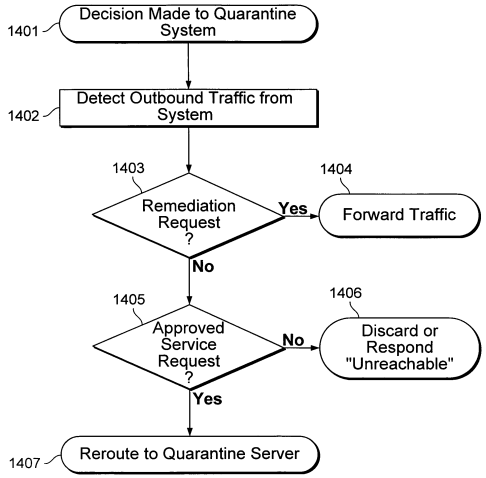
| Claim | Exemplary Citation from Roskind |
|---|---|
| | detected (1203) then an apparent infestation is noted (1204) in this example. In some embodiments, a response to infestation may include quarantining of the computer or network containing the computer, for example as discussed in conjunction with FIGS. 14, 15, and 16. In some embodiments, a response to infestation may include an attempt to remediate the problem, for example by inoculation, such as discussed in conjunction with FIG. 17. If no anomaly is detected (1203) then monitoring is complete (1205) in this example. In some embodiments, monitoring for anomalous traffic may be continuous. In some embodiments, monitoring for anomalous traffic may be periodic. For example, periodic monitoring may consist of monitoring some number of computers, such as 1 computer, for some period of time, such as 2 minutes, and then not monitoring those computers again for another period of time, such as 1. hour. As another example, periodic monitoring may be randomized, for example by changing the duration of monitoring, pattern of selecting computers to monitor, and/or the unmonitored duration, to be difficult or impossible to predict, for example by being driven by a pseudo random number generator, subject to restrictions of available monitoring computers."<br><br>Roskind at 13:54-14:26:<br>"FIG. 13 is a flow diagram of a method for monitoring one or more computers for infestation according to some embodiments. In this example monitoring of a computer for infestation begins (1301), for example by retrieving a list of one or more addresses of computers, such as addresses of participating subscribers. In some embodiments, this list may be a list of addresses for some or all subscribers for a given ISP. In some embodiments, the list may be a list of IP addresses issued by a DHCP server, such as on a LAN, or a list of IP addresses observed by a router, such as a router on a LAN, or complete list of IP addresses in a given subnet. A computer associated with an address identified in a list is queried for a cleanliness assertion (1302), for example by contacting a trusted computing base within a computer, and requesting an authenticated infestation scan by trusted software. An example of a trusted computing base within a computer is the Paladium security initiative under development by Microsoft and supported by Intel and American Micro Devices. Another example of a trusted computing base is described in various TCG specifications, such as the TCG Architecture Overview, published by the Trusted Computing Group. Trusted code bases may for example execute antivirus scans of the remainder of the computer, including untrusted portions of the disk and/or operating system. In some embodiments, trusted code bases may digitally sign assertions about the cleanliness (e.g. infestation status) and/or state of their computers. In some embodiments, |

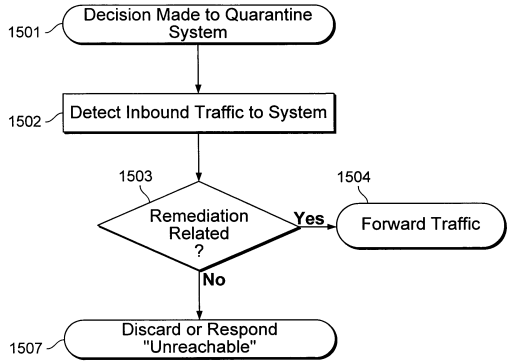
| Claim | Exemplary Citation from Roskind |
|---|---|
| | the query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus. software, with assertions about the currency of a scan, such as the last time a scan was performed, or a version associated with a current anti-contagion software or definition file in use, wherein a sufficiently updated software and/or scan may act as a cleanliness assertion. In some embodiments, an operating system may respond with information associated with its patch level, wherein a sufficiently recent patch level may be interpreted as an assertion of cleanliness. If a computer asserts it is clean (1303) then monitoring is complete (1305) in this example. If a cleanliness assertion is not provided (1303) then an infestation or vulnerability is presumed (1304) in this example."<br><br>Roskind at 14:27-15:12:<br>"FIG. 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with FIG. 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. In some embodiments, requests for a quarantine may be made on an individual computer via settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic. is tested in this example to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation. Rerouting of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of rerouting a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example."<br><br>Roskind at 15:36-56:<br>"In some embodiments, a configuration based quarantine during an installation of an operating system, such as Microsoft Windows, may be automatically setup, for example by a default installation setting up restrictions in a firewall installed with the OS or by an installation setting defaults for use when network connectivity is enabled, that establishes a quarantine, for example restricting internet connections, for example allowing internet connections only to a security. update site such as Microsoft Windows Update. In some embodiments, settings that may establish a quarantine, such as default settings in an operating system installation, may be altered programmatically to remove the quarantine in response to a remediation site, such as a security update service such as Microsoft Windows Update, asserting that there are no other security updates pending. In some embodiments, configuration settings that may establish a quarantine may be altered programmatically to enable a quarantine in response to the presence of one or more security updates, such as provided by an operating system update service such as Microsoft Windows Update, that are available for installation on a computer." |
| **[7]** The method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device. | Roskind discloses and/or renders obvious the method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device.<br><br>Roskind at 11:15-56:<br>"FIG. 10A is a flow diagram of a method for identifying and remedying problems according to some embodiments. A problem may be identified as some event or status that may cause direct or potential |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | harm. Exemplary problems include vulnerability or infestation. In this example, a problem such as a vulnerability or infestation is detected (1001). Infestation herein refers to the current presence and/or execution of contagion. In some embodiments, detection may be made by a router, firewall, or other network component, separately or in concert, using techniques such as those illustrated by FIGS. 11, 12, and 13. In some embodiments, detection may be made by a computing device, for example a computing device operated by an ISP. After a detection of a problem, a computer or network containing the problem is quarantined (1002). In some embodiments, quarantining includes preventing unauthorized communications from being sent from the quarantined computer, such as efforts to infect, probe, or harass other computers, or efforts to communicate data without authorization, including for example file contents and keyboard entry logs. In some embodiments, no communications are authorized. In some embodiments, quarantining includes preventing undesired communications from reaching the quarantined computer, such as control messages or infectious messages. Examples of quarantining activities are illustrated in FIGS. 14 and 15. In this example, the quarantined computer is provided access to remediation services (1003). In some embodiments, access to remediation includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor's server, or providing virus and worm disinfecting tools, such as focused removal tools, or data updates for previously installed repair tools. In some embodiments, access to remediation includes allowing direct access to vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained. In some embodiments, access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443, certain content requests, such as specific URLs or specific file downloads. In some embodiments, remediation content may be substituted for other requested content, for example as discussed in conjunction with FIG. 14."<br><br>Roskind at 14:27-15:12:<br>"FIG. 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with FIG. 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. In some embodiments, requests for a quarantine may be made on an individual computer via settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic. is tested in this example to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation. Rerouting of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of rerouting a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example."<br><br>Roskind at 15:13-35:<br>"FIG. 15 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1501), for example as described in conjunction with 1401 of FIG. 14. Inbound traffic originally destined for a quarantined computer is detected (1502), for example by a network device such as by a router. An example of detecting |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | inbound traffic destined for a quarantined computer is to have a list of quarantined IP addresses, and filter or provide additional processing on traffic destined for an address on the list. Detected inbound traffic is tested in this example to see if it is remediation related (1503), such as a response to a remediation request. Direct responses to remediation requests may for example be identified using stateful packet inspection firewall techniques known to those skilled in the art. In various embodiments, at least certain types of traffic from approved sites such as anti-contagion vendors, security update providers, and/or internal ISP sites are deemed remediation related. If traffic is remediation related (1503) then it is forwarded to the quarantined computer (1504) in this example. If traffic is not remediation related (1503) then, in this example, it is discarded or responded to with a message indicating that the destination is unreachable (1507)."<br><br>Figure 14<br><br><br>FIG. 14 |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Figure 15<br><br><br>FIG. 15 |
| **[8pre].** A computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor to perform: | Roskind discloses and/or renders obvious a computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor<br><br>*See*, claim 1, above.<br><br>*See also, e.g.,*<br><br>Roskind at 2:47-60:<br>"The invention can be implemented in numerous ways, including as a process, an apparatus, a system, a composition of matter, a computer readable medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or electronic communication links. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. A component such as a processor or a memory described as being configured to perform a task includes both a general component that is temporarily configured to perform the task at a given time and a specific component that is |

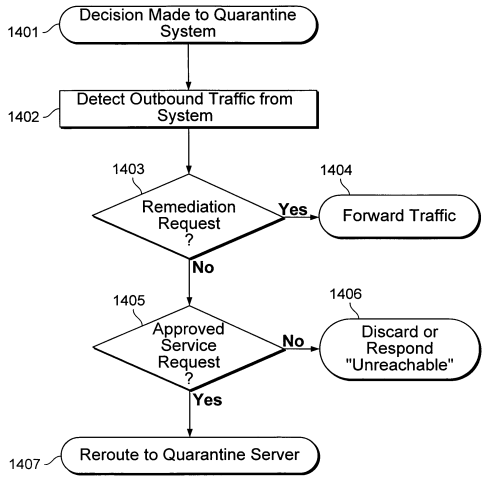
| Claim | Exemplary Citation from Roskind |
|---|---|
| | manufactured to perform the task. In general, the order of the steps of disclosed processes may be altered within the scope of the invention." |
| **[8a].** a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises: | Roskind discloses and/or renders obvious a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises.<br><br>*See* [1b]. |
| **[8b(a)]** restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment; | Roskind discloses and/or renders obvious restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment.<br><br>*See* [1b(a)]. |
| **[8b(b)]** restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and | Roskind discloses and/or renders obvious restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols.<br><br>*See* [1b(b)]. |
| **[8c].** rendering a web page to display on the client device from the network | Roskind discloses and/or renders obvious rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client |

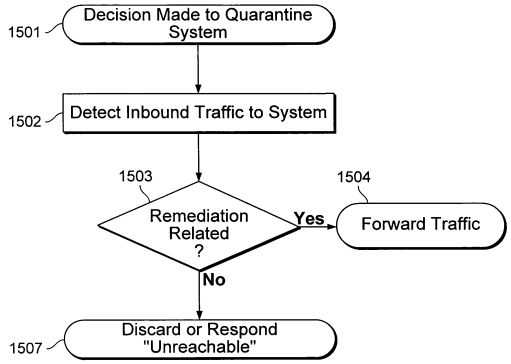
| Claim | Exemplary Citation from Roskind |
|---|---|
| access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to the implementation of one of the plurality of quarantine control function of the client device. | device to perform an action in order to obtain unrestricted access to the Internet responsive to the implementation of one of the plurality of quarantine control function of the client device.<br><br>*See* [1c]. |
| **[13]** The computer program product of claim 8, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment. | Roskind discloses and/or renders obvious the computer program product of claim 8, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment.<br><br>*See* [1(b)(a)]. |
| **[14]** The computer program product of claim 8, wherein the instructions are further translatable by the at least one processor to perform: all of the plurality of quarantine control functions over the client device. | Roskind discloses and/or renders obvious the computer program product of claim 8, wherein the instructions are further translatable by the at least one processor to perform: all of the plurality of quarantine control functions over the client device.<br><br>*E.g.*: |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Roskind at 11:15-56:<br>"FIG. 10A is a flow diagram of a method for identifying and remedying problems according to some embodiments. A problem may be identified as some event or status that may cause direct or potential harm. Exemplary problems include vulnerability or infestation. In this example, a problem such as a vulnerability or infestation is detected (1001). Infestation herein refers to the current presence and/or execution of contagion. In some embodiments, detection may be made by a router, firewall, or other network component, separately or in concert, using techniques such as those illustrated by FIGS. 11, 12, and 13. In some embodiments, detection may be made by a computing device, for example a computing device operated by an ISP. After a detection of a problem, a computer or network containing the problem is quarantined (1002). In some embodiments, quarantining includes preventing unauthorized communications from being sent from the quarantined computer, such as efforts to infect, probe, or harass other computers, or efforts to communicate data without authorization, including for example file contents and keyboard entry logs. In some embodiments, no communications are authorized. In some embodiments, quarantining includes preventing undesired communications from reaching the quarantined computer, such as control messages or infectious messages. Examples of quarantining activities are illustrated in FIGS. 14 and 15. In this example, the quarantined computer is provided access to remediation services (1003). In some embodiments, access to remediation includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor's server, or providing virus and worm disinfecting tools, such as focused removal tools, or data updates for previously installed repair tools. In some embodiments, access to remediation includes allowing direct access to vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained. In some embodiments, access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443, certain content requests, such as specific URLs or specific file downloads. In some embodiments, remediation content may be substituted for other requested content, for example as discussed in conjunction with FIG. 14.<br><br>Roskind at 14:27-15:12:<br>"FIG. 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with FIG. 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. In some embodiments, requests for a quarantine may be made on an individual computer via settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic. is tested in this example to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation. Rerouting of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of rerouting a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example." |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Roskind at 15:13-35:<br>"FIG. 15 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1501), for example as described in conjunction with 1401 of FIG. 14. Inbound traffic originally destined for a quarantined computer is detected (1502), for example by a network device such as by a router. An example of detecting inbound traffic destined for a quarantined computer is to have a list of quarantined IP addresses, and filter or provide additional processing on traffic destined for an address on the list. Detected inbound traffic is tested in this example to see if it is remediation related (1503), such as a response to a remediation request. Direct responses to remediation requests may for example be identified using stateful packet inspection firewall techniques known to those skilled in the art. In various embodiments, at least certain types of traffic from approved sites such as anti-contagion vendors, security update providers, and/or internal ISP sites are deemed remediation related. If traffic is remediation related (1503) then it is forwarded to the quarantined computer (1504) in this example. If traffic is not remediation related (1503) then, in this example, it is discarded or responded to with a message indicating that the destination is unreachable (1507)." |

| Claim | Exemplary Citation from Roskind |
| --- | --- |
| | Figure 14   FIG. 14 |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Figure 15<br><br><br>FIG. 15 |
| **[15pre].** A network access gateway device, comprising: | Roskind discloses and/or renders obvious a network access gateway device, comprising:<br><br>*See* [1a]. |
| **[15a].** at least one processor; and | Roskind discloses and/or renders obvious at least one processor.<br><br>*See* [1a]. |
| **[15b].** at least one non-transitory computer readable medium storing instructions translatable by the at least one processor to perform: | Roskind discloses and/or renders obvious at least one non-transitory computer readable medium storing instructions translatable by the at least one processor to perform:<br><br>*See* [1a]. |
| **[15c].** a plurality of quarantine control functions | Roskind discloses and/or renders obvious a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is |

| Claim | Exemplary Citation from Roskind |
|---|---|
| over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises: | between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises:<br><br>*See* [8a]. |
| **[15c(a)]** restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment; | Roskind discloses and/or renders obvious restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment.<br><br>*See* [1b(a)]. |
| **[15c(b)]** restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and | Roskind discloses and/or renders obvious restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols.<br><br>*See* [1b(b)]. |
| **[15d].** rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to | Roskind discloses and/or renders obvious rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device.<br><br>*See* [1c]. |

| Claim | Exemplary Citation from Roskind |
|---|---|
| perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device. | |
| **[16]** The system of claim 15, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses. | Roskind discloses and/or renders obvious the system of claim 15, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses.<br><br>*See* [2]. |
| **[17]** The system of claim 15, wherein the instructions are further translatable by the at least one processor to perform:<br>evaluating network traffic emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert. | Roskind discloses and/or renders obvious the system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: evaluating network traffic emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert.<br><br>*E.g.*,:<br><br>Roskind at 13:10-53:<br>"FIG. 12 is a flow diagram of a method for identifying an infestation according to some embodiments. In this example, a device near a computer, such as a firewall on a LAN or an ISP's router, is used in some embodiments to monitor a computer for infestation (1201). Network traffic is monitored for anomalous traffic volume, port, or IP destination (1202), for example by detecting large volumes of outbound traffic, such as email traffic or instant messaging traffic. Another example of anomalous traffic is a TCP/IP connection to a server that is known to control a collection of infested machines, in a way that suggests the connecting machine is controlled by the server, such as connecting and transmitting an assertion that it is controlled or available to comply. Another example |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | of anomalous traffic is a connection to a computer that is a current target of a denial of service attack, with a pattern that is consistent with the attack, such as a connection to a targeted port, or the use of a falsified return IP address. In some embodiments, a falsified return address may be detected by a router, such as an ISP router, that is aware that the return address is not on the sourcing subnet, or not associated with the MAC address that has supplied the corresponding packets. If an anomaly is detected (1203) then an apparent infestation is noted (1204) in this example. In some embodiments, a response to infestation may include quarantining of the computer or network containing the computer, for example as discussed in conjunction with FIGS. 14, 15, and 16. In some embodiments, a response to infestation may include an attempt to remediate the problem, for example by inoculation, such as discussed in conjunction with FIG. 17. If no anomaly is detected (1203) then monitoring is complete (1205) in this example. In some embodiments, monitoring for anomalous traffic may be continuous. In some embodiments, monitoring for anomalous traffic may be periodic. For example, periodic monitoring may consist of monitoring some number of computers, such as 1 computer, for some period of time, such as 2 minutes, and then not monitoring those computers again for another period of time, such as 1. hour. As another example, periodic monitoring may be randomized, for example by changing the duration of monitoring, pattern of selecting computers to monitor, and/or the unmonitored duration, to be difficult or impossible to predict, for example by being driven by a pseudo random number generator, subject to restrictions of available monitoring computers."<br><br>Roskind at 13:54-14:26:<br>"FIG. 13 is a flow diagram of a method for monitoring one or more computers for infestation according to some embodiments. In this example monitoring of a computer for infestation begins (1301), for example by retrieving a list of one or more addresses of computers, such as addresses of participating subscribers. In some embodiments, this list may be a list of addresses for some or all subscribers for a given ISP. In some embodiments, the list may be a list of IP addresses issued by a DHCP server, such as on a LAN, or a list of IP addresses observed by a router, such as a router on a LAN, or complete list of IP addresses in a given subnet. A computer associated with an address identified in a list is queried for a cleanliness assertion (1302), for example by contacting a trusted computing base within a computer, and requesting an authenticated infestation scan by trusted software. An example of a trusted computing base within a computer is the Paladium security initiative under development by Microsoft and supported by Intel and American Micro Devices. |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Another example of a trusted computing base is described in various TCG specifications, such as the TCG Architecture Overview, published by the Trusted Computing Group. Trusted code bases may for example execute antivirus scans of the remainder of the computer, including untrusted portions of the disk and/or operating system. In some embodiments, trusted code bases may digitally sign assertions about the cleanliness (e.g. infestation status) and/or state of their computers. In some embodiments, the query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus. software, with assertions about the currency of a scan, such as the last time a scan was performed, or a version associated with a current anti-contagion software or definition file in use, wherein a sufficiently updated software and/or scan may act as a cleanliness assertion. In some embodiments, an operating system may respond with information associated with its patch level, wherein a sufficiently recent patch level may be interpreted as an assertion of cleanliness. If a computer asserts it is clean (1303) then monitoring is complete (1305) in this example. If a cleanliness assertion is not provided (1303) then an infestation or vulnerability is presumed (1304) in this example."<br><br>Roskind at 14:27-15:12:<br>"FIG. 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with FIG. 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. In some embodiments, requests for a quarantine may be made on an individual computer via settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic. is tested in this example to see if it is associated with a remediation request (1403), |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation. Rerouting of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of rerouting a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example."<br><br>Roskind at 15:36-56:<br>"In some embodiments, a configuration based quarantine during an installation of an operating system, such as Microsoft Windows, may be automatically setup, for example by a default installation setting up restrictions in a firewall installed with the OS or by an installation setting defaults for use when network connectivity is enabled, that establishes a quarantine, for example restricting internet connections, for example allowing internet connections only to a security. update site such as Microsoft Windows Update. In some embodiments, settings that may establish a quarantine, such as default settings in an operating system installation, may be altered programmatically to remove the quarantine in response to a remediation site, such as a security update service such as Microsoft Windows Update, asserting that there are no other security updates pending. In some embodiments, configuration settings that may establish a quarantine may be altered programmatically to enable a quarantine in response to the presence of one or more security updates, such as provided by an operating system update service such as Microsoft Windows Update, that are available for installation on a computer." |

| Claim | Exemplary Citation from Roskind |
|---|---|
| **[18]** The system of claim 15, wherein the instructions are further translatable by the at least one processor to perform:<br>filtering the network traffic emanating from the client device to limit network packet flow by the client device. | Roskind discloses and/or renders obvious the system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: filtering the network traffic emanating from the client device to limit network packet flow by the client device.<br><br>*E.g.*<br><br>Roskind at 1:14-43:<br>"Unwanted and/or malicious network communications, such as spam, phishing, worm propagation, etc., hamper productivity and the use and enjoyment of computer and network resources by end users, burden affected networks with unauthorized and/or undesired traffic, and expose recipients to the risk of theft, fraud, etc. Current technologies for dealing with such unauthorized and/or unwanted communications focus on filtering messages at a point in the communication path close to the recipient system, such as anti-spam and/or other security software installed on the destination host and/or a local mail (or other messaging) server to which communications, to the destination host are directed for delivery to the destination host, e.g., by detecting messages sent by blacklisted senders and/or messages containing header or other content that indicates the message is suspicious. While this approach can be an effective way to protect an individual host or a group of destination hosts served by a local server, it does not address the network congestion problem and leaves vulnerable hosts not protected by destination (or destination mail or messaging server) based filtering software. In addition, in many cases an attacker causes each of one or more compromised hosts to send multiple instances of a malicious communication, often simultaneously or nearly so, magnifying the effect on the network. Therefore, there is a need for an effective way to intercept and take corrective action with respect to unauthorized, unwanted, and/or otherwise malicious electronic mail and/or other network communications that better protects the network and provides protection to destination hosts that are not protected by destination or destination mail or messaging server based filtering software."<br><br>Roskind at 15:13-35:<br>"FIG. 15 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1501), for example as described in conjunction with 1401 of FIG. 14. Inbound traffic originally destined for a quarantined computer is detected (1502), for example by a network device such as by a router. An example of detecting |

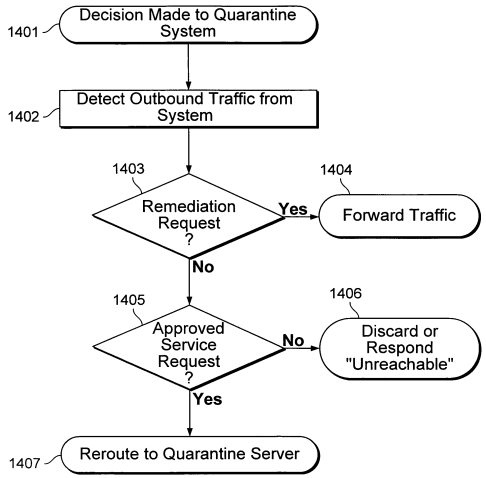
| Claim | Exemplary Citation from Roskind |
|---|---|
| | inbound traffic destined for a quarantined computer is to have a list of quarantined IP addresses, and filter or provide additional processing on traffic destined for an address on the list. Detected inbound traffic is tested in this example to see if it is remediation related (1503), such as a response to a remediation request. Direct responses to remediation requests may for example be identified using stateful packet inspection firewall techniques known to those skilled in the art. In various embodiments, at least certain types of traffic from approved sites such as anti-contagion vendors, security update providers, and/or internal ISP sites are deemed remediation related. If traffic is remediation related (1503) then it is forwarded to the quarantined computer (1504) in this example. If traffic is not remediation related (1503) then, in this example, it is discarded or responded to with a message indicating that the destination is unreachable (1507)."<br><br>Roskind at 15:36-56:<br>"In some embodiments, a configuration based quarantine during an installation of an operating system, such as Microsoft Windows, may be automatically setup, for example by a default installation setting up restrictions in a firewall installed with the OS or by an installation setting defaults for use when network connectivity is enabled, that establishes a quarantine, for example restricting internet connections, for example allowing internet connections only to a security. update site such as Microsoft Windows Update. In some embodiments, settings that may establish a quarantine, such as default settings in an operating system installation, may be altered programmatically to remove the quarantine in response to a remediation site, such as a security update service such as Microsoft Windows Update, asserting that there are no other security updates pending. In some embodiments, configuration settings that may establish a quarantine may be altered programmatically to enable a quarantine in response to the presence of one or more security updates, such as provided by an operating system update service such as Microsoft Windows Update, that are available for installation on a computer."<br><br>Roskind at 15:57-16:43:<br>"FIG. 16 is a flow diagram of a method for a quarantine server to respond to requests according to some embodiments. In this example, a quarantine server is started (1601), for example by starting a web server, or DNS server, or proxy server, or ftp server, or some combination server. The server waits for a request (1602), for example by listening on a port and waiting for a connection. In some embodiments, a device such as a router may forward outbound traffic from a quarantined computer to |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | a quarantine server, for example as illustrated in conjunction with 1407 of FIG. 14. If a received connection is a web server request (1603), such as an HTTP request, then the server responds with a quarantine notification page (1604) in this example. An example of a quarantine notification page is a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain. The links on the quarantine notification page may be examples of HTTP addresses that are for use in remediation. Another example of a quarantine notification page is a page that redirects to a quarantine notification page. If the request is not a web server request (1603), then it is tested to see if it is a DNS inquiry (1605) in this example. A DNS inquiry may for example appear on port 53 using TCP/IP or UDP. If the request is not a DNS inquiry (1605) then it may be discarded or responded to as "unreachable" (1606) in this example. If the request is a DNS inquiry (1605) then, in this example, the inquiry is tested to see if it is a DNS request for a remediation host name (1608). A remediation host name may include a host name as appropriate to the reason for a quarantine, such as a host providing anti-contagion software, or a host providing security updates, or a host internal to (or partnered with) an ISP. If the DNS inquiry was for a remediation host name (1608) then the request is proxied to an external DNS service provider (1609) in this example. A proxy to a DNS service (1609) may return a stored or cached response, such as the actual IP address of the host name, or it may contact an external DNS service to relay back the proposed IP address. If the DNS inquiry was not for a remediation host name (1608) then an IP address for a quarantine server is provided (1607) in this example. In some embodiments, when a redirected IP address is provided, such as that of a quarantine server, the DNS response may include a short time to live, for example 0 seconds. A short time to live ensures that a further DNS query will be sent prior to subsequent communications being sent from the quarantined computer to the host that was the subject of the DNS query, aiding a return to normal routing of traffic once the computer is no longer under quarantine. In some embodiments, the server(s) in this example may continue to wait for a service request (1602) in parallel with the processing of the requests as described above, or may wait for a service request again after disposition of the previous request as described above." |
| **[19]** The system of claim 15, wherein the instructions are further translatable by | Roskind discloses and/or renders obvious the system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: routing the network traffic emanating from the client device to limit network packet traversal by the client device. |

| Claim | Exemplary Citation from Roskind |
|---|---|
| the at least one processor to perform:<br>routing the network traffic emanating from the client device to limit network packet traversal by the client device. | *E.g.*:<br><br>Roskind at 11:57-12:13:<br>"FIG. 10B is a block diagram illustrating a network environment in which infected hosts and/or networks are quarantined according to some embodiments. A plurality of hosts 1 to "m", represented in FIG. 10B by hosts 1020, 1022, and 1024, connect via a router 1026 and a gateway 1028 to the Internet 1030. In various embodiments the router 1026 is omitted or included in the gateway 1028. In various embodiments, gateway 1028 comprises a gateway, router, firewall, or other device configured to provide and control access between a protected network and the Internet and/or another public or private network. In various embodiments, the pro cess of FIG. 10A is implemented, in the event of quarantine of one or more of hosts 1020-1024, for example, on the affected (quarantined) host, router 1026, and/or gateway 1028. In some embodiments, a quarantined host (or a host associated with a quarantined network or sub-network) is permitted to access a remediation server 1032, e.g., to download a patch, more current threat definition, etc. In some embodiments, requests to connection to a host other than the remediation server 1032 are redirected to a quarantine server 1034 configured to provide a notice and/or other information and/or instructions to a user of the quarantined host. In various alternative embodiments the quarantine server 1034 is omitted or resides on the router 1026 and/or gateway 1028."<br><br>Roskind at 14:27-15:12:<br>"FIG. 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with FIG. 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. In some embodiments, requests for a quarantine may be made on an individual computer via settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic. is tested in this example to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation. Rerouting of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of rerouting a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example."<br><br>Roskind at 15:57-16:43:<br>"FIG. 16 is a flow diagram of a method for a quarantine server to respond to requests according to some embodiments. In this example, a quarantine server is started (1601), for example by starting a web server, or DNS server, or proxy server, or ftp server, or some combination server. The server waits for a request (1602), for example by listening on a port and waiting for a connection. In some embodiments, a device such as a router may forward outbound traffic from a quarantined computer to a quarantine server, for example as illustrated in conjunction with 1407 of FIG. 14. If a received connection is a web server request (1603), such as an HTTP request, then the server responds with a quarantine notification page (1604) in this example. An example of a quarantine notification page is a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | software for removing a virus that the quarantined computer is believed to contain. The links on the quarantine notification page may be examples of HTTP addresses that are for use in remediation. Another example of a quarantine notification page is a page that redirects to a quarantine notification page. If the request is not a web server request (1603), then it is tested to see if it is a DNS inquiry (1605) in this example. A DNS inquiry may for example appear on port 53 using TCP/IP or UDP. If the request is not a DNS inquiry (1605) then it may be discarded or responded to as "unreachable" (1606) in this example. If the request is a DNS inquiry (1605) then, in this example, the inquiry is tested to see if it is a DNS request for a remediation host name (1608). A remediation host name may include a host name as appropriate to the reason for a quarantine, such as a host providing anti-contagion software, or a host providing security updates, or a host internal to (or partnered with) an ISP. If the DNS inquiry was for a remediation host name (1608) then the request is proxied to an external DNS service provider (1609) in this example. A proxy to a DNS service (1609) may return a stored or cached response, such as the actual IP address of the host name, or it may contact an external DNS service to relay back the proposed IP address. If the DNS inquiry was not for a remediation host name (1608) then an IP address for a quarantine server is provided (1607) in this example. In some embodiments, when a redirected IP address is provided, such as that of a quarantine server, the DNS response may include a short time to live, for example 0 seconds. A short time to live ensures that a further DNS query will be sent prior to subsequent communications being sent from the quarantined computer to the host that was the subject of the DNS query, aiding a return to normal routing of traffic once the computer is no longer under quarantine. In some embodiments, the server(s) in this example may continue to wait for a service request (1602) in parallel with the processing of the requests as described above, or may wait for a service request again after disposition of the previous request as described above." |

| Claim | Exemplary Citation from Roskind |
|---|---|
| | Figure 14<br><br><br>FIG. 14 |
| **[20]** The system of claim 15, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment. | Roskind discloses and/or renders obvious the system of claim 15, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment.<br><br>*See* [1b(a)] |

**Ex. B-2 - Invalidity of U.S. Patent No. 8,543,710 against US20030191966 to Gleichauf ("Gleichauf")**

Fortinet, Inc. ("Fortinet") provides this chart subject to all reservations, objections, statements, and disclaimers set forth herein and in Fortinet's Preliminary Invalidity Contentions Cover Pleading, as well as any amendment, supplement, or modification thereof, which are incorporated herein by reference in their entirety.

On information and belief, and subject to further investigation and discovery, Gleichauf was published on October 9, 2003, and is thus available as prior art under at least pre-AIA §102(a).

As illustrated in the chart below, Gleichauf anticipates the asserted claims of the '710 Patent. To the extent Gleichauf is found not to expressly disclose certain limitations in the asserted claims, such limitations are inherent. To the extent Gleichauf is found not to anticipate any asserted claims or claim elements of the '710 Patent, the reference nevertheless renders those claims or claim elements obvious under 35 U.S.C. § 103, either alone or in combination with other art identified in the cover pleading or herein. These Preliminary Invalidity Contentions are not an admission by Fortinet that the accused products, including any current or past versions of the accused products, are covered by, or infringe the asserted claims, but are based instead on the recognition that if the claims are interpreted to be broad enough to encompass the accused products, the claims must also be construed to have that same scope when considering whether they are invalid.

The following chart is partially based on, but is not limited by, the claim constructions implicit in Plaintiff's Infringement Contentions, to the extent that such constructions are apparent from the Infringement Contentions. Fortinet notes that in many instances, Plaintiff's Infringement Contentions fail to provide adequate notice of Plaintiff's construction of the asserted claims and fail to comply with the Court's scheduling order and other applicable rules. Fortinet does not accept the assumptions concerning the scope and meaning implicit in Plaintiff's Infringement Contentions, to the extent those assumptions are discernible, and reserves the right to challenge Plaintiff's proposed (or implied) constructions. Fortinet also reserves the right to revise and supplement these charts if and when Plaintiff is permitted to provide revised Infringement Contentions or otherwise make its positions known. To the extent that these Preliminary Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the asserted claims, Fortinet does not necessarily advocate any such construction as proper constructions of those terms or phrase. Fortinet also reserves the right to revise and supplement these charts after the Court construes the claims. Citations given in the chart below are merely representative of the respective elements and are not meant to be exhaustive.



Netskope, Ex. 2003
Fortinet v. Netskope, IPR2026-00042

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| **[1pre]** A method of network traffic quarantine control, comprising: | Gleichauf discloses and/or renders obvious a method of network traffic quarantine control.<br><br>*E.g.*:<br><br>Gleichauf at [0006]:<br>"Some embodiments of the present invention provide a number of technical advantages. For example, according to one embodiment of the present invention a network management controller is provided that operates to immediately disable the communications capability of a rogue (or an infected computer) that contains an infective element by removing its corresponding address. This prohibits the rogue from communicating to a next computer or to another destination, which may infect additional elements within the network. The network management controller allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is important because time is a critical element in containing infective elements once they have penetrated the corresponding security system."<br><br>Gleichauf at [0018]:<br>"In accordance with the teachings of the present invention, communication system 10 provides an architecture for identifying infective element 12 after it has been introduced into the architecture of communication system 10 . Communication system 10 also provides the ability to pinpoint or otherwise recognize the location of infective element 12 as within infected computer 18 . In implementing a communications protocol, computers 16 a , 16 b , and 16 c offer a peer monitoring feature that detects damaging elements, such as infective element 12 , as they enter communication system 10 . Accordingly, a cooperative signaling approach is provided for computers 16 a , 16 b , and 16 c , whereby infected computer 18 is targeted as a rogue, i.e., inclusive of some malicious file, corrupt data segment, or non-compliant operation, which may cause harm to components within communication system 10 ."<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further."<br><br>Gleichauf at [0020]:<br>"This community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is particularly critical in network security systems where time is of the essence in containing damaging information, such as infective element 12 , once a security breach has occurred within communication system 10 . In addition, communication system 10 offers the benefit of peer monitoring, whereby only a selected number of peers within the network community need to be properly configured in order to identify a rogue within the system architecture. Network management controller 14 may respond to the identification of infective element 12 with any number of appropriate remedies (as described in greater detail below) in order to prohibit infective element 12 from permeating through the system being threatened." |
| **[1a]** at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network; | Gleichauf discloses and/or renders obvious at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network.<br><br>*E.g.*:<br><br>Gleichauf at [0017]:<br>"FIG. 1 is a block diagram of a communication system 10 for detecting an infective element 12 in a network environment in accordance with one embodiment of the present invention. Communication system 10 includes a network management controller 14 , multiple computers 16 a 16 d , an infected computer 18 , an external network 22 , and an internal network 24 . Additionally, communication system 10 includes an external website 28 , a remediator website 30 , an authentication server 34 , and a policies node 38 ." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | Gleichauf at [0018]:<br>"In accordance with the teachings of the present invention, communication system 10 provides an architecture for identifying infective element 12 after it has been introduced into the architecture of communication system 10 . Communication system 10 also provides the ability to pinpoint or otherwise recognize the location of infective element 12 as within infected computer 18 . In implementing a communications protocol, computers 16 a , 16 b , and 16 c offer a peer monitoring feature that detects damaging elements, such as infective element 12 , as they enter communication system 10 . Accordingly, a cooperative signaling approach is provided for computers 16 a , 16 b , and 16 c , whereby infected computer 18 is targeted as a rogue, i.e., inclusive of some malicious file, corrupt data segment, or non-compliant operation, which may cause harm to components within communication system 10 ."<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further."<br><br>Gleichauf at [0036]:<br>"FIG. 2B is a block diagram that illustrates another example implementation network management controller 14 in which a switch 46 is coupled to network management controller 14 . Network management controller 14 may be coupled to switch 46 directly or indirectly, or alternatively switch 46 may be positioned within network management controller 14 . Switch 46 operates to receive one or more data packets from a communicating device and communicates those data packets to selected locations within communication system 10 . In addition, switch 46 may receive one or more data packets from external network 22 , policies node 38 , or any other suitable element or device within or external to communication system 10 in order to communicate information to one or more elements within communication system 10 ." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | Gleichauf at [0037]:<br>"FIG. 2C is a block diagram illustrating another example implementation of network management controller 14 . A firewall 48 may be coupled to network management controller 14 and may operate to discard, delete, or otherwise avoid damaging data segments sought to be communicated to any element or device within communication system 10 . Alternatively, firewall 48 may be inclusive of network management controller 14 or coupled indirectly to network management controller 14 where appropriate. Firewall 48 is a system architecture that enforces an access control policy between two nodes, such as a virtual private network (VPN) and a public node, such as the Internet. A VPN is a private data network that makes use of the public network infrastructure. A VPN network may provide secured sharing of public sources for data by using encryption techniques to ensure that only authorized users can view or “tunnel" into a company's private networking files."<br><br>Gleichauf at [0038]:<br>"Firewall 48 may determine which inside services or elements can be accessed from outside sources and which outside services and elements can be accessed by inside sources. In essence, firewall 48 may be viewed as a pair of tools that block and permit communications traffic. Firewall 48 may also provide a single choke point where security functions or audits (such as audits based on policies stored in policies node 38 ) may be imposed. Firewall 48 may also provide a network administrator with data associated with what kinds or what amount of traffic has passed through it and how many attempts were made to break through the firewall architecture. Firewall 48 may also hide information about a network to which it is coupled and make it seem as though all outgoing traffic originates from firewall 48 rather than from internal network 24 ."<br><br>Gleichauf at [0039]:<br>"Referring back to FIG. 1, computers 16 a 16 d and infected computer 18 each represent a device that accepts information in the form of digital data and manipulates that information for some result based on a program or on a sequence of instructions. In a particular embodiment of the present invention, computers 16 a 16 d each represent a desktop central processing unit that may receive and communicate data within communication system 10 . Alternatively, computers 16 a 16 d and infected computer 18 may be any other suitable device for the communication of data. For example, computers 16 a 16 d and infected computer 18 may be a cellular or wireless telephone, a personal digital assistance (PDA), a laptop or an electronic notebook, or any other device, component, or |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | object capable of initiating voice or data exchanges within communication system 10 . Computers 16 a 16 d and infecting computer 18 may additionally provide an interface to the human user, such as via microphone, display, keyboard, or other terminal equipment such as an interface to a personal computer or to a facsimile machine in cases where computers 16 a 16 d and infected computer 18 are used as a modem. Computers 16 a 16 d , and infected computer 18 may also be a database or a program capable of facilitating a data exchange between two nodes. Data, as used herein, refers to any type of numeric, voice, video or script data, or any other suitable information in any appropriate format that may be communicated from one point to another."<br><br>Gleichauf at [0040]:<br>"Computers 16 a and 16 b are illustrated in FIG. 1 as being included in a subset of computers particular to an engineering unit or an engineering division within a company or an entity. In addition, computer 16 c is illustrated as associated with an accounting unit or division within an entity. Each of computers 16 a 16 d , as well as infected computer 18 , are coupled to internal network 24 such that they may exchange data or otherwise interact in a network environment."<br><br>Gleichauf at [0049]:<br>"External network 22 represents a series of points or nodes of interconnected communication paths for receiving and transmitting packets of information that propagate through communication system 10 . External network 22 may offer a communications interface between a node, such as external website 28 , and any element connected to internal network 24 . External network 22 may be any local area network (LAN), metropolitan area network (MAN) or wide area network (WAN), or any other appropriate architecture or system that facilitates communications in a mesh (wireless) network or in other suitable network environments. External network 22 implements a transmission control protocol/internet protocol (TCP/IP) communication language protocol in a particular embodiment of the present invention; however, external network 22 may alternatively implement any other suitable communication protocol for transmitting and receiving data packets within communication system 10." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | Gleichauf at [0050]:<br>"Internal network 24 represents an internal architecture that provides a communicative interface to one or more network components within communication system 10 . Internal network 24 allows computers 16 a d , infected computer 18 , network management controller 14 , and remediator website 30 to interact with each other in a network environment. In addition, internal network 24 may provide a communicative interface for any other elements or components within or external to communication system 10 . Internal network 24 is a VPN in a particular embodiment of the present invention; however internal network 24 may alternatively by any LAN, MAN, WAN, or any other architecture system that facilitates communications in a network environment. Internal network 24 implements a TCP/IP communication language protocol in a particular embodiment of the present invention; however, internal network 24 may alternatively implement any other suitable communication protocol for transmitting and receiving data packets within communication system 10." |
| **[1b]** at the network access gateway device, performing a plurality of quarantine control functions over the client device, wherein the plurality of quarantine control functions comprises: | Gleichauf discloses and/or renders obvious at the network access gateway device, performing a plurality of quarantine control functions over the client device.<br><br>*E.g.*,:<br><br>Gleichauf at [0017]:<br>"FIG. 1 is a block diagram of a communication system 10 for detecting an infective element 12 in a network environment in accordance with one embodiment of the present invention. Communication system 10 includes a network management controller 14 , multiple computers 16 a 16 d , an infected computer 18 , an external network 22 , and an internal network 24 . Additionally, communication system 10 includes an external website 28 , a remediator website 30 , an authentication server 34 , and a policies node 38 ."<br><br>Gleichauf at [0018]:<br>"In accordance with the teachings of the present invention, communication system 10 provides an architecture for identifying infective element 12 after it has been introduced into the architecture of |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | communication system 10 . Communication system 10 also provides the ability to pinpoint or otherwise recognize the location of infective element 12 as within infected computer 18 . In implementing a communications protocol, computers 16 a , 16 b , and 16 c offer a peer monitoring feature that detects damaging elements, such as infective element 12 , as they enter communication system 10 . Accordingly, a cooperative signaling approach is provided for computers 16 a , 16 b , and 16 c , whereby infected computer 18 is targeted as a rogue, i.e., inclusive of some malicious file, corrupt data segment, or non-compliant operation, which may cause harm to components within communication system 10 ."<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further."<br><br>Gleichauf at [0020]:<br>"This community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is particularly critical in network security systems where time is of the essence in containing damaging information, such as infective element 12 , once a security breach has occurred within communication system 10 . In addition, communication system 10 offers the benefit of peer monitoring, whereby only a selected number of peers within the network community need to be properly configured in order to identify a rogue within the system architecture. Network management controller 14 may respond to the identification of infective element 12 with any number of appropriate remedies (as described in greater detail below) in order to prohibit infective element 12 from permeating through the system being threatened." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | Gleichauf at [0032]:<br>"In accordance with a particular embodiment of the present invention, network management controller 14 may remove or reassign the IP address of infected computer 18 such that the communicating capability of infected computer 18 is disabled. Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30 . Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols. In addition, network management controller 14 may generate an alert signal to be broadcast to any element that might interact with infected computer 18 . The alert signal may include information such as: the address (or the IP address) of infected computer 18 , the type of damaging element present in the network, or remedial measures for dealing with an encounter with infected computer 18 ."<br><br>Gleichauf at [0037]:<br>"FIG. 2C is a block diagram illustrating another example implementation of network management controller 14 . A firewall 48 may be coupled to network management controller 14 and may operate to discard, delete, or otherwise avoid damaging data segments sought to be communicated to any element or device within communication system 10 . Alternatively, firewall 48 may be inclusive of network management controller 14 or coupled indirectly to network management controller 14 where appropriate. Firewall 48 is a system architecture that enforces an access control policy between two nodes, such as a virtual private network (VPN) and a public node, such as the Internet. A VPN is a private data network that makes use of the public network infrastructure. A VPN network may provide secured sharing of public sources for data by using encryption techniques to ensure that only authorized users can view or “tunnel" into a company's private networking files."<br><br>Gleichauf at [0038]:<br>"Firewall 48 may determine which inside services or elements can be accessed from outside sources and which outside services and elements can be accessed by inside sources. In essence, firewall 48 may be viewed as a pair of tools that block and permit communications traffic. Firewall 48 may also provide a single choke point where security functions or audits (such as audits based on policies stored in policies node 38 ) may be imposed. Firewall 48 may also provide a network administrator |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | with data associated with what kinds or what amount of traffic has passed through it and how many attempts were made to break through the firewall architecture. Firewall 48 may also hide information about a network to which it is coupled and make it seem as though all outgoing traffic originates from firewall 48 rather than from internal network 24 ."<br><br>Gleichauf at [0039]:<br>"Referring back to FIG. 1, computers 16 a 16 d and infected computer 18 each represent a device that accepts information in the form of digital data and manipulates that information for some result based on a program or on a sequence of instructions. In a particular embodiment of the present invention, computers 16 a 16 d each represent a desktop central processing unit that may receive and communicate data within communication system 10 . Alternatively, computers 16 a 16 d and infected computer 18 may be any other suitable device for the communication of data. For example, computers 16 a 16 d and infected computer 18 may be a cellular or wireless telephone, a personal digital assistance (PDA), a laptop or an electronic notebook, or any other device, component, or object capable of initiating voice or data exchanges within communication system 10 . Computers 16 a 16 d and infecting computer 18 may additionally provide an interface to the human user, such as via microphone, display, keyboard, or other terminal equipment such as an interface to a personal computer or to a facsimile machine in cases where computers 16 a 16 d and infected computer 18 are used as a modem. Computers 16 a 16 d , and infected computer 18 may also be a database or a program capable of facilitating a data exchange between two nodes. Data, as used herein, refers to any type of numeric, voice, video or script data, or any other suitable information in any appropriate format that may be communicated from one point to another."<br><br>Gleichauf at [0040]:<br>"Computers 16 a and 16 b are illustrated in FIG. 1 as being included in a subset of computers particular to an engineering unit or an engineering division within a company or an entity. In addition, computer 16 c is illustrated as associated with an accounting unit or division within an entity. Each of computers 16 a 16 d , as well as infected computer 18 , are coupled to internal network 24 such that they may exchange data or otherwise interact in a network environment." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| **[1b(a)]** restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment; | Gleichauf discloses and/or renders obvious restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment.<br><br>*E.g.*,:<br><br>Claim 17:<br>"The method of claim 15, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Claim 26:<br>"The method of claim 24, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Claim 54:<br>"The software of claim 52, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Gleichauf at [0008]:<br>"Yet another advantage of one embodiment of the present invention is that a computer containing an infective element may be directed to a remediator website in order to comply with a network security enforcement protocol. The remediator website may then facilitate the removal of the infective element from the component suspected of including damaging information. The suspected component may continue to communicate with the remediator website until it removes the infective element or until it is otherwise cured or deemed in proper compliance with existing security |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | protocols, at which time it may be permitted to resume communications with other network components."<br><br>Gleichauf at [0017]:<br>"FIG. 1 is a block diagram of a communication system 10 for detecting an infective element 12 in a network environment in accordance with one embodiment of the present invention. Communication system 10 includes a network management controller 14 , multiple computers 16 a 16 d , an infected computer 18 , an external network 22 , and an internal network 24 . Additionally, communication system 10 includes an external website 28 , a remediator website 30 , an authentication server 34 , and a policies node 38 ."<br><br>Gleichauf at [0018]:<br>"In accordance with the teachings of the present invention, communication system 10 provides an architecture for identifying infective element 12 after it has been introduced into the architecture of communication system 10 . Communication system 10 also provides the ability to pinpoint or otherwise recognize the location of infective element 12 as within infected computer 18 . In implementing a communications protocol, computers 16 a , 16 b , and 16 c offer a peer monitoring feature that detects damaging elements, such as infective element 12 , as they enter communication system 10 . Accordingly, a cooperative signaling approach is provided for computers 16 a , 16 b , and 16 c , whereby infected computer 18 is targeted as a rogue, i.e., inclusive of some malicious file, corrupt data segment, or non-compliant operation, which may cause harm to components within communication system 10 ."<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | Gleichauf at [0020]:<br>"This community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is particularly critical in network security systems where time is of the essence in containing damaging information, such as infective element 12 , once a security breach has occurred within communication system 10 . In addition, communication system 10 offers the benefit of peer monitoring, whereby only a selected number of peers within the network community need to be properly configured in order to identify a rogue within the system architecture. Network management controller 14 may respond to the identification of infective element 12 with any number of appropriate remedies (as described in greater detail below) in order to prohibit infective element 12 from permeating through the system being threatened."<br><br>Gleichauf at [0052]:<br>"Remediator website 30 is a security element designed to facilitate the removal of infective element 12 from infected computer 18 in accordance with one embodiment of the present invention. Remediator website 30 is coupled to internal network 24 and infected computer 18 , and may receive a communication from infected computer 18 after it has been identified as a rogue, i.e. inclusive of a damaging element. Infected computer 18 may be shunted or otherwise directed to remediator website 30 until the proper software or configurations are downloaded or until infective element 12 is removed from infected computer 18 . Remediator website 30 may include hardware, software, or any other object or element that combats or that facilitates the removal of infective element 12 . Alternatively, where infected computer 18 has been erroneously directed to remediator website 30 , remediator website 30 may evaluate infected computer 18 and determine that it is in proper security compliance and accordingly permit infected computer 18 to further communicate within communication system 10 ."<br><br>Gleichauf at [0061]:<br>"From step 104 , the signal may be responded to in various ways as illustrated by steps 106 and 108 . At step 106 , the signal is received and a communicating capability of infected computer 18 may be disabled. The disablement may include removing or reassigning the address associated with infected computer 18 . Alternatively, at step 108 infected computer 18 may be disabled by employing sandboxing, constraining, isolating, or siderailing techniques as described above. In addition, |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | communications may be avoided by network components forewarned of potential harmful elements, items, or agents communicated by infected computer 18 . Network management controller 14 may also execute any number of other actions in order to prohibit infected computer 18 from further communications. For example, network management controller 14 may access polices node 38 in order to restrict some service offered to infected computer 18 or invoke policies node 38 in removing the IP address of infected computer 18 . In addition, network management controller 14 may broadcast an alert signal to components within communication system 10 to beware of communications from infected computer 18 ." |
| **[1b(b)]** restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and | Gleichauf discloses and/or renders obvious restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols.<br><br>*E.g.*:<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further."<br><br>Gleichauf at [0032]:<br>"In accordance with a particular embodiment of the present invention, network management controller 14 may remove or reassign the IP address of infected computer 18 such that the communicating capability of infected computer 18 is disabled. Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30 . Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols. In |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | addition, network management controller 14 may generate an alert signal to be broadcast to any element that might interact with infected computer 18 . The alert signal may include information such as: the address (or the IP address) of infected computer 18 , the type of damaging element present in the network, or remedial measures for dealing with an encounter with infected computer 18 ."<br><br>Gleichauf at [0033]:<br>"In a particular embodiment of the present invention, network management controller 14 may leverage or otherwise control dynamic host configuration protocol (DHCP) services in order to disable infected computer 18. The DHCP protocol represents a platform that lets a network operator to centrally manage (and to automate where appropriate) the assignment of IP addressing configurations within a communication system 10. Without the DHCP configuration, an IP address must be entered manually at each entity or system wishing to communicate in the network environment. DHCP also allows network management controller 14 to supervise and to distribute IP addresses from a central point."<br><br>Gleichauf at [0034]:<br>"End users, such as those using computers 16 a 16 d , may have an assigned IP address that is static or dynamically assigned from a pool of addresses. End users may then register for selected services provided within the network. These services may be stored in polices node 38 . These services may include internet services, intranet services, and other various services such as push services or priority services offered to an end user. Network management controller 14 may gain control of the IP address granted to an end user when that end user logs on to internal network 24 . Control of the IP address provides an executive power to network management controller 14 because an invalid IP address effectively disables a communicating capability of an associated device within communication system 10 ."<br><br>Gleichauf at [0036]:<br>"FIG. 2B is a block diagram that illustrates another example implementation network management controller 14 in which a switch 46 is coupled to network management controller 14 . Network management controller 14 may be coupled to switch 46 directly or indirectly, or alternatively switch 46 may be positioned within network management controller 14 . Switch 46 operates to receive one or more data packets from a communicating device and communicates those data packets to selected |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | locations within communication system 10 . In addition, switch 46 may receive one or more data packets from external network 22 , policies node 38 , or any other suitable element or device within or external to communication system 10 in order to communicate information to one or more elements within communication system 10 ."<br><br>Gleichauf at [0037]:<br>"FIG. 2C is a block diagram illustrating another example implementation of network management controller 14 . A firewall 48 may be coupled to network management controller 14 and may operate to discard, delete, or otherwise avoid damaging data segments sought to be communicated to any element or device within communication system 10 . Alternatively, firewall 48 may be inclusive of network management controller 14 or coupled indirectly to network management controller 14 where appropriate. Firewall 48 is a system architecture that enforces an access control policy between two nodes, such as a virtual private network (VPN) and a public node, such as the Internet. A VPN is a private data network that makes use of the public network infrastructure. A VPN network may provide secured sharing of public sources for data by using encryption techniques to ensure that only authorized users can view or “tunnel" into a company's private networking files."<br><br>Gleichauf at [0038]:<br>"Firewall 48 may determine which inside services or elements can be accessed from outside sources and which outside services and elements can be accessed by inside sources. In essence, firewall 48 may be viewed as a pair of tools that block and permit communications traffic. Firewall 48 may also provide a single choke point where security functions or audits (such as audits based on policies stored in policies node 38 ) may be imposed. Firewall 48 may also provide a network administrator with data associated with what kinds or what amount of traffic has passed through it and how many attempts were made to break through the firewall architecture. Firewall 48 may also hide information about a network to which it is coupled and make it seem as though all outgoing traffic originates from firewall 48 rather than from internal network 24 ."<br><br>Gleichauf at [0057]:<br>"Policies node 38 is a data storage element that includes protocols that dictate what may be accessed and run by elements within communication system 10 . Policies node 38 may be coupled to network management controller 14 and may communicate information thereto, which enables network |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | management controller 14 to implement policies based on the specific restrictions or capabilities of computers 16 a 16 d . The policies included within policies node 38 may be items such as: quality of service, access/authorization privileges, high availability, priority, or any other suitable network enhancement or communications feature."<br><br>Gleichauf at [0058]:<br>"In a particular embodiment of the present invention, network management controller 14 may access policies node 38 in order to retrieve information about the services provided to each of computers 16 a 16 d and infected computer 18 . In the case where infected element 18 is discovered as inclusive of infective element 12 , network management controller 14 may access policies node 38 in order to disable one or more of those policies or services being provided to infected 18 until it properly complies with the requisite security parameters. This allows network management controller 14 yet another way to address infected computer 18 once infective element 12 is discovered within communication system 10 . Thus, policies node 38 offers the ability to directly effect a policy relating to infected computer 18 , which is sought to be restricted because of the presence of a damaging element."<br><br>Gleichauf at [0061]:<br>"From step 104 , the signal may be responded to in various ways as illustrated by steps 106 and 108 . At step 106 , the signal is received and a communicating capability of infected computer 18 may be disabled. The disablement may include removing or reassigning the address associated with infected computer 18 . Alternatively, at step 108 infected computer 18 may be disabled by employing sandboxing, constraining, isolating, or siderailing techniques as described above. In addition, communications may be avoided by network components forewarned of potential harmful elements, items, or agents communicated by infected computer 18 . Network management controller 14 may also execute any number of other actions in order to prohibit infected computer 18 from further communications. For example, network management controller 14 may access polices node 38 in order to restrict some service offered to infected computer 18 or invoke policies node 38 in removing the IP address of infected computer 18 . In addition, network management controller 14 may broadcast an alert signal to components within communication system 10 to beware of communications from infected computer 18 ." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| **[1c]** rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device. | Gleichauf discloses and/or renders obvious rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device.<br>*E.g.*:<br><br>Claim 26:<br>"The method of claim 24, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Claim 54:<br>"The software of claim 52, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Gleichauf at [0008]:<br>"Yet another advantage of one embodiment of the present invention is that a computer containing an infective element may be directed to a remediator website in order to comply with a network security enforcement protocol. The remediator website may then facilitate the removal of the infective element from the component suspected of including damaging information. The suspected component may continue to communicate with the remediator website until it removes the infective element or until it is otherwise cured or deemed in proper compliance with existing security protocols, at which time it may be permitted to resume communications with other network components."<br><br>Gleichauf at [0032]:<br>"In accordance with a particular embodiment of the present invention, network management controller 14 may remove or reassign the IP address of infected computer 18 such that the communicating capability of infected computer 18 is disabled. Network management controller 14 |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30 . Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols. In addition, network management controller 14 may generate an alert signal to be broadcast to any element that might interact with infected computer 18 . The alert signal may include information such as: the address (or the IP address) of infected computer 18 , the type of damaging element present in the network, or remedial measures for dealing with an encounter with infected computer 18 ."<br><br>Gleichauf at [0035]:<br>"Network management controller 14 may be coupled to, or implemented in conjunction with, any number of networking devices or elements within communication system 10 . FIGS. 2 A2 C illustrate a number of example implementations in which network management controller 14 may be leveraged with existing network equipment. For example, network management controller 14 may be coupled to a router 44 as illustrated in FIG. 2A. Alternatively, network management controller 14 may be inclusive of router 44 or indirectly coupled to router 44 where appropriate. Router 44 is a device or a piece of software that determines the next network point to which a packet of information is directed in communication system 10 . Router 44 may be coupled to any other network component within communication system 10 or to another router where appropriate. Additionally, router 44 may be positioned at a gateway or at a communications interface in order to direct packets of information from one point to the next. Router 44 may receive data packets from computers 16 a 16 d and infected computer 18 and communicate those packets to external network 22 . In addition, router 44 may receive data packets from external network 22 , such as via external website 28 , and communicate those packets of information back to one or more computers 16 a 16 d and infected computer 18 ."<br><br>Gleichauf at [0036]:<br>"FIG. 2B is a block diagram that illustrates another example implementation network management controller 14 in which a switch 46 is coupled to network management controller 14 . Network management controller 14 may be coupled to switch 46 directly or indirectly, or alternatively switch 46 may be positioned within network management controller 14 . Switch 46 operates to receive one |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | or more data packets from a communicating device and communicates those data packets to selected locations within communication system 10 . In addition, switch 46 may receive one or more data packets from external network 22 , policies node 38 , or any other suitable element or device within or external to communication system 10 in order to communicate information to one or more elements within communication system 10 ."<br><br>Gleichauf at [0037]:<br>"FIG. 2C is a block diagram illustrating another example implementation of network management controller 14 . A firewall 48 may be coupled to network management controller 14 and may operate to discard, delete, or otherwise avoid damaging data segments sought to be communicated to any element or device within communication system 10 . Alternatively, firewall 48 may be inclusive of network management controller 14 or coupled indirectly to network management controller 14 where appropriate. Firewall 48 is a system architecture that enforces an access control policy between two nodes, such as a virtual private network (VPN) and a public node, such as the Internet. A VPN is a private data network that makes use of the public network infrastructure. A VPN network may provide secured sharing of public sources for data by using encryption techniques to ensure that only authorized users can view or “tunnel" into a company's private networking files."<br><br>Gleichauf at [0038]:<br>"Firewall 48 may determine which inside services or elements can be accessed from outside sources and which outside services and elements can be accessed by inside sources. In essence, firewall 48 may be viewed as a pair of tools that block and permit communications traffic. Firewall 48 may also provide a single choke point where security functions or audits (such as audits based on policies stored in policies node 38 ) may be imposed. Firewall 48 may also provide a network administrator with data associated with what kinds or what amount of traffic has passed through it and how many attempts were made to break through the firewall architecture. Firewall 48 may also hide information about a network to which it is coupled and make it seem as though all outgoing traffic originates from firewall 48 rather than from internal network 24 ."<br><br>Gleichauf at [0052]:<br>"Remediator website 30 is a security element designed to facilitate the removal of infective element 12 from infected computer 18 in accordance with one embodiment of the present invention. |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | Remediator website 30 is coupled to internal network 24 and infected computer 18 , and may receive a communication from infected computer 18 after it has been identified as a rogue, i.e. inclusive of a damaging element. Infected computer 18 may be shunted or otherwise directed to remediator website 30 until the proper software or configurations are downloaded or until infective element 12 is removed from infected computer 18 . Remediator website 30 may include hardware, software, or any other object or element that combats or that facilitates the removal of infective element 12 . Alternatively, where infected computer 18 has been erroneously directed to remediator website 30 , remediator website 30 may evaluate infected computer 18 and determine that it is in proper security compliance and accordingly permit infected computer 18 to further communicate within communication system 10 ."<br><br>Gleichauf at [0063]:<br>"Additionally, although numerous components, such as network management controller 14 or communication protocol shim 42 , have been illustrated in designated positions of communication system 10 , these elements may be placed in any suitable location or within any appropriate structure such that the cooperative signaling approach of the present invention is achieved. Numerous other changes, substitutions, variations, alterations, and modifications may be suggested to one skilled in the art, and it is intended that the present invention encompass all such changes, substitutions, variations, alterations, and modifications as following within the spirit and scope of the appended claims." |
| **[2]** The method according to claim 1, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses. | Gleichauf discloses and/or renders obvious the method according to claim 1, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses.<br><br>*E.g.*:<br><br>Claim 46:<br>"The software of claim 44, wherein the communicating capability of the second computer is disabled by directing the second computer to software for removing the infective element from the second computer." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | Claim 54:<br>"The software of claim 52, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Gleichauf at [0032]:<br>"In accordance with a particular embodiment of the present invention, network management controller 14 may remove or reassign the IP address of infected computer 18 such that the communicating capability of infected computer 18 is disabled. Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30 . Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols. In addition, network management controller 14 may generate an alert signal to be broadcast to any element that might interact with infected computer 18 . The alert signal may include information such as: the address (or the IP address) of infected computer 18 , the type of damaging element present in the network, or remedial measures for dealing with an encounter with infected computer 18 ."<br><br>Gleichauf at [0045]:<br>"In operation, once a damaging element is detected, communication protocol shim 42 may send a signal directly to infected computer 18 that signifies that infective element 12 is within its internal structure. Infected computer 18 may then respond to the signal by communicating with remediator website 30 , or alternatively by performing some cleaning or security check for its corresponding internal structure."<br><br>Gleichauf at [0052]:<br>"Remediator website 30 is a security element designed to facilitate the removal of infective element 12 from infected computer 18 in accordance with one embodiment of the present invention. Remediator website 30 is coupled to internal network 24 and infected computer 18 , and may receive |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | a communication from infected computer 18 after it has been identified as a rogue, i.e. inclusive of a damaging element. Infected computer 18 may be shunted or otherwise directed to remediator website 30 until the proper software or configurations are downloaded or until infective element 12 is removed from infected computer 18 . Remediator website 30 may include hardware, software, or any other object or element that combats or that facilitates the removal of infective element 12 . Alternatively, where infected computer 18 has been erroneously directed to remediator website 30 , remediator website 30 may evaluate infected computer 18 and determine that it is in proper security compliance and accordingly permit infected computer 18 to further communicate within communication system 10 ." |
| **[6]** The method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment. | Gleichauf discloses and/or renders obvious the method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment.<br>*E.g.*:<br><br>Claim 26:<br>"The method of claim 24, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Gleichauf at [0017]:<br>"FIG. 1 is a block diagram of a communication system 10 for detecting an infective element 12 in a network environment in accordance with one embodiment of the present invention. Communication system 10 includes a network management controller 14 , multiple computers 16 a 16 d , an infected computer 18 , an external network 22 , and an internal network 24 . Additionally, communication system 10 includes an external website 28 , a remediator website 30 , an authentication server 34 , and a policies node 38 ."<br><br>Gleichauf at [0018]:<br>"In accordance with the teachings of the present invention, communication system 10 provides an architecture for identifying infective element 12 after it has been introduced into the architecture of |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | communication system 10 . Communication system 10 also provides the ability to pinpoint or otherwise recognize the location of infective element 12 as within infected computer 18 . In implementing a communications protocol, computers 16 a , 16 b , and 16 c offer a peer monitoring feature that detects damaging elements, such as infective element 12 , as they enter communication system 10 . Accordingly, a cooperative signaling approach is provided for computers 16 a , 16 b , and 16 c , whereby infected computer 18 is targeted as a rogue, i.e., inclusive of some malicious file, corrupt data segment, or non-compliant operation, which may cause harm to components within communication system 10 ."<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further."<br><br>Gleichauf at [0020]:<br>"This community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is particularly critical in network security systems where time is of the essence in containing damaging information, such as infective element 12 , once a security breach has occurred within communication system 10 . In addition, communication system 10 offers the benefit of peer monitoring, whereby only a selected number of peers within the network community need to be properly configured in order to identify a rogue within the system architecture. Network management controller 14 may respond to the identification of infective element 12 with any number of appropriate remedies (as described in greater detail below) in order to prohibit infective element 12 from permeating through the system being threatened." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | Gleichauf at [0032]:<br>"In accordance with a particular embodiment of the present invention, network management controller 14 may remove or reassign the IP address of infected computer 18 such that the communicating capability of infected computer 18 is disabled. Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30 . Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols. In addition, network management controller 14 may generate an alert signal to be broadcast to any element that might interact with infected computer 18 . The alert signal may include information such as: the address (or the IP address) of infected computer 18 , the type of damaging element present in the network, or remedial measures for dealing with an encounter with infected computer 18 ."<br><br>Gleichauf at [0052]:<br>"Remediator website 30 is a security element designed to facilitate the removal of infective element 12 from infected computer 18 in accordance with one embodiment of the present invention. Remediator website 30 is coupled to internal network 24 and infected computer 18 , and may receive a communication from infected computer 18 after it has been identified as a rogue, i.e. inclusive of a damaging element. Infected computer 18 may be shunted or otherwise directed to remediator website 30 until the proper software or configurations are downloaded or until infective element 12 is removed from infected computer 18 . Remediator website 30 may include hardware, software, or any other object or element that combats or that facilitates the removal of infective element 12 . Alternatively, where infected computer 18 has been erroneously directed to remediator website 30 , remediator website 30 may evaluate infected computer 18 and determine that it is in proper security compliance and accordingly permit infected computer 18 to further communicate within communication system 10 ." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| **[7]** The method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device. | Gleichauf discloses and/or renders obvious the method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device.<br><br>Claim 26:<br>"The method of claim 24, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Claim 54:<br>"The software of claim 52, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Gleichauf at [0017]:<br>"FIG. 1 is a block diagram of a communication system 10 for detecting an infective element 12 in a network environment in accordance with one embodiment of the present invention. Communication system 10 includes a network management controller 14 , multiple computers 16 a 16 d , an infected computer 18 , an external network 22 , and an internal network 24 . Additionally, communication system 10 includes an external website 28 , a remediator website 30 , an authentication server 34 , and a policies node 38 ."<br><br>Gleichauf at [0018]:<br>"In accordance with the teachings of the present invention, communication system 10 provides an architecture for identifying infective element 12 after it has been introduced into the architecture of communication system 10 . Communication system 10 also provides the ability to pinpoint or otherwise recognize the location of infective element 12 as within infected computer 18 . In implementing a communications protocol, computers 16 a , 16 b , and 16 c offer a peer monitoring feature that detects damaging elements, such as infective element 12 , as they enter communication system 10 . Accordingly, a cooperative signaling approach is provided for computers 16 a , 16 b , and |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | 16 c , whereby infected computer 18 is targeted as a rogue, i.e., inclusive of some malicious file, corrupt data segment, or non-compliant operation, which may cause harm to components within communication system 10 ."<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further."<br><br>Gleichauf at [0020]:<br>"This community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is particularly critical in network security systems where time is of the essence in containing damaging information, such as infective element 12 , once a security breach has occurred within communication system 10 . In addition, communication system 10 offers the benefit of peer monitoring, whereby only a selected number of peers within the network community need to be properly configured in order to identify a rogue within the system architecture. Network management controller 14 may respond to the identification of infective element 12 with any number of appropriate remedies (as described in greater detail below) in order to prohibit infective element 12 from permeating through the system being threatened."<br><br>Gleichauf at [0032]:<br>"In accordance with a particular embodiment of the present invention, network management controller 14 may remove or reassign the IP address of infected computer 18 such that the communicating capability of infected computer 18 is disabled. Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30 . Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols. In addition, network management controller 14 may generate an alert signal to be broadcast to any element that might interact with infected computer 18 . The alert signal may include information such as: the address (or the IP address) of infected computer 18 , the type of damaging element present in the network, or remedial measures for dealing with an encounter with infected computer 18 ."<br><br>Gleichauf at [0061]:<br>"From step 104 , the signal may be responded to in various ways as illustrated by steps 106 and 108 . At step 106 , the signal is received and a communicating capability of infected computer 18 may be disabled. The disablement may include removing or reassigning the address associated with infected computer 18 . Alternatively, at step 108 infected computer 18 may be disabled by employing sandboxing, constraining, isolating, or siderailing techniques as described above. In addition, communications may be avoided by network components forewarned of potential harmful elements, items, or agents communicated by infected computer 18 . Network management controller 14 may also execute any number of other actions in order to prohibit infected computer 18 from further communications. For example, network management controller 14 may access polices node 38 in order to restrict some service offered to infected computer 18 or invoke policies node 38 in removing the IP address of infected computer 18 . In addition, network management controller 14 may broadcast an alert signal to components within communication system 10 to beware of communications from infected computer 18 ." |
| **[8pre].** A computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor to perform: | Gleichauf discloses and/or renders obvious a computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor to perform:<br><br>*See* [1pre]-[1a]. |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| **[8a].** a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises: | Gleichauf discloses and/or renders obvious a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises.<br><br>*See* [1b]. |
| **[8b(a)]** restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment; | Gleichauf discloses and/or renders obvious restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment.<br><br>*See* [1b(a)]. |
| **[8b(b)]** restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and | Gleichauf discloses and/or renders obvious restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols.<br><br>*See* [1b(b)]. |
| **[8c].** rendering a web page to display on the client device from the network access gateway device, wherein the web page | Gleichauf discloses and/or renders obvious rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to the implementation of one of the plurality of quarantine control function of the client device. |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to the implementation of one of the plurality of quarantine control function of the client device. | *See* [1c]. |
| **[13]** The computer program product of claim 8, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment. | Gleichauf discloses and/or renders obvious the computer program product of claim 8, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment.<br><br>*See* [1(b)(a)]. |
| **[14]** The computer program product of claim 8, wherein the instructions are further translatable by the at least one processor to perform: all of the plurality of quarantine control functions over the client device. | Gleichauf discloses and/or renders obvious the computer program product of claim 8, wherein the instructions are further translatable by the at least one processor to perform: all of the plurality of quarantine control functions over the client device.<br><br>*E.g.*:<br><br>Claim 26:<br>"The method of claim 24, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Claim 54:<br>"The software of claim 52, wherein the communicating capability of the second computer is disabled by directing the second computer to a remediator website until the infective element is removed from the second computer, the remediator website operable to facilitate removal of the infective element from the second computer."<br><br>Gleichauf at [0017]:<br>"FIG. 1 is a block diagram of a communication system 10 for detecting an infective element 12 in a network environment in accordance with one embodiment of the present invention. Communication system 10 includes a network management controller 14 , multiple computers 16 a 16 d , an infected computer 18 , an external network 22 , and an internal network 24 . Additionally, communication system 10 includes an external website 28 , a remediator website 30 , an authentication server 34 , and a policies node 38 ."<br><br>Gleichauf at [0018]:<br>"In accordance with the teachings of the present invention, communication system 10 provides an architecture for identifying infective element 12 after it has been introduced into the architecture of communication system 10 . Communication system 10 also provides the ability to pinpoint or otherwise recognize the location of infective element 12 as within infected computer 18 . In implementing a communications protocol, computers 16 a , 16 b , and 16 c offer a peer monitoring feature that detects damaging elements, such as infective element 12 , as they enter communication system 10 . Accordingly, a cooperative signaling approach is provided for computers 16 a , 16 b , and 16 c , whereby infected computer 18 is targeted as a rogue, i.e., inclusive of some malicious file, corrupt data segment, or non-compliant operation, which may cause harm to components within communication system 10 ."<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further."<br>Gleichauf at [0020]:<br>"This community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is particularly critical in network security systems where time is of the essence in containing damaging information, such as infective element 12 , once a security breach has occurred within communication system 10 . In addition, communication system 10 offers the benefit of peer monitoring, whereby only a selected number of peers within the network community need to be properly configured in order to identify a rogue within the system architecture. Network management controller 14 may respond to the identification of infective element 12 with any number of appropriate remedies (as described in greater detail below) in order to prohibit infective element 12 from permeating through the system being threatened."<br><br>Gleichauf at [0032]:<br>"In accordance with a particular embodiment of the present invention, network management controller 14 may remove or reassign the IP address of infected computer 18 such that the communicating capability of infected computer 18 is disabled. Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30 . Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols. In addition, network management controller 14 may generate an alert signal to be broadcast to any element that might interact with infected computer 18 . The alert signal may include information such as: the address (or the IP address) of infected computer 18 , the type of damaging element present in the network, or remedial measures for dealing with an encounter with infected computer 18 ." |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | Gleichauf at [0061]:<br>"From step 104 , the signal may be responded to in various ways as illustrated by steps 106 and 108 . At step 106 , the signal is received and a communicating capability of infected computer 18 may be disabled. The disablement may include removing or reassigning the address associated with infected computer 18 . Alternatively, at step 108 infected computer 18 may be disabled by employing sandboxing, constraining, isolating, or siderailing techniques as described above. In addition, communications may be avoided by network components forewarned of potential harmful elements, items, or agents communicated by infected computer 18 . Network management controller 14 may also execute any number of other actions in order to prohibit infected computer 18 from further communications. For example, network management controller 14 may access polices node 38 in order to restrict some service offered to infected computer 18 or invoke policies node 38 in removing the IP address of infected computer 18 . In addition, network management controller 14 may broadcast an alert signal to components within communication system 10 to beware of communications from infected computer 18 ." |
| **[15pre].** A network access gateway device, comprising: | Gleichauf discloses and/or renders obvious a network access gateway device, comprising:<br><br>*See* [1a]. |
| **[15a].** at least one processor; and | Gleichauf discloses and/or renders obvious at least one processor.<br><br>*See* [1a]. |
| **[15b].** at least one non-transitory computer readable medium storing instructions translatable by the at least one processor to perform: | Gleichauf discloses and/or renders obvious at least one non-transitory computer readable medium storing instructions translatable by the at least one processor to perform:<br><br>*See* [1a]. |
| **[15c].** a plurality of quarantine control functions | Gleichauf discloses and/or renders obvious a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises: | between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises:<br><br>*See* [8a]. |
| **[15c(a)]** restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment; | Gleichauf discloses and/or renders obvious restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment.<br><br>*See* [1b(a)]. |
| **[15c(b)]** restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and | Gleichauf discloses and/or renders obvious restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols.<br><br>*See* [1b(b)]. |
| **[15d].** rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to | Gleichauf discloses and/or renders obvious rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device.<br><br>*See* [1c]. |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device. | |
| **[16]** The system of claim 15, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses. | Gleichauf discloses and/or renders obvious the system of claim 15, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses.<br><br>*See* [2]. |
| **[17]** The system of claim 15, wherein the instructions are further translatable by the at least one processor to perform:<br>evaluating network traffic emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert. | Gleichauf discloses and/or renders obvious the system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: evaluating network traffic emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert.<br><br>*See* [3]. |
| **[18]** The system of claim 15, wherein the instructions are further translatable by the at least one processor to | Gleichauf discloses and/or renders obvious the system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: filtering the network traffic emanating from the client device to limit network packet flow by the client device. |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| perform: filtering the network traffic emanating from the client device to limit network packet flow by the client device. | *E.g.*,:<br><br>Claim 27:<br>"The method of claim 24, further comprising: receiving, by a third computer, the signal; identifying the address of the second computer such that communications from the second computer are recognized; and rejecting, by the third computer, the communications from the second computer until the infective element is removed from the second computer."<br>Claim 55:<br>"The software of claim 52, further operable to: receive, by a third computer, the signal; identify the address of the second computer such that communications from the second computer are recognized; and reject, by the third computer, the communications from the second computer until the infective element is removed from the second computer."<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further."<br><br>Gleichauf at [0020]:<br>"This community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is particularly critical in network security systems where time is of the essence in containing damaging information, such as infective element 12 , once a security breach has occurred within communication system 10 . In addition, communication system 10 offers the benefit of peer monitoring, whereby only a selected number of peers within the network community need to be properly configured in order to identify a rogue within the system architecture. Network management controller 14 may respond to the identification of infective element 12 with any number of appropriate remedies (as described in greater detail |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | below) in order to prohibit infective element 12 from permeating through the system being threatened."<br><br>Gleichauf at [0032]:<br>"In accordance with a particular embodiment of the present invention, network management controller 14 may remove or reassign the IP address of infected computer 18 such that the communicating capability of infected computer 18 is disabled. Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30 . Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols. In addition, network management controller 14 may generate an alert signal to be broadcast to any element that might interact with infected computer 18 . The alert signal may include information such as: the address (or the IP address) of infected computer 18 , the type of damaging element present in the network, or remedial measures for dealing with an encounter with infected computer 18 ."<br><br>Gleichauf at [0035]:<br>"Network management controller 14 may be coupled to, or implemented in conjunction with, any number of networking devices or elements within communication system 10 . FIGS. 2 A2 C illustrate a number of example implementations in which network management controller 14 may be leveraged with existing network equipment. For example, network management controller 14 may be coupled to a router 44 as illustrated in FIG. 2A. Alternatively, network management controller 14 may be inclusive of router 44 or indirectly coupled to router 44 where appropriate. Router 44 is a device or a piece of software that determines the next network point to which a packet of information is directed in communication system 10 . Router 44 may be coupled to any other network component within communication system 10 or to another router where appropriate. Additionally, router 44 may be positioned at a gateway or at a communications interface in order to direct packets of information from one point to the next. Router 44 may receive data packets from computers 16 a 16 d and infected computer 18 and communicate those packets to external network 22 . In addition, router 44 may receive data packets from external network 22 , such as via external website 28 , and |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | communicate those packets of information back to one or more computers 16 a 16 d and infected computer 18 ."<br><br>Gleichauf at [0036]:<br>"FIG. 2B is a block diagram that illustrates another example implementation network management controller 14 in which a switch 46 is coupled to network management controller 14 . Network management controller 14 may be coupled to switch 46 directly or indirectly, or alternatively switch 46 may be positioned within network management controller 14 . Switch 46 operates to receive one or more data packets from a communicating device and communicates those data packets to selected locations within communication system 10 . In addition, switch 46 may receive one or more data packets from external network 22 , policies node 38 , or any other suitable element or device within or external to communication system 10 in order to communicate information to one or more elements within communication system 10 ."<br><br>Gleichauf at [0037]:<br>"FIG. 2C is a block diagram illustrating another example implementation of network management controller 14 . A firewall 48 may be coupled to network management controller 14 and may operate to discard, delete, or otherwise avoid damaging data segments sought to be communicated to any element or device within communication system 10 . Alternatively, firewall 48 may be inclusive of network management controller 14 or coupled indirectly to network management controller 14 where appropriate. Firewall 48 is a system architecture that enforces an access control policy between two nodes, such as a virtual private network (VPN) and a public node, such as the Internet. A VPN is a private data network that makes use of the public network infrastructure. A VPN network may provide secured sharing of public sources for data by using encryption techniques to ensure that only authorized users can view or “tunnel" into a company's private networking files." |
| **[19]** The system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: routing the network traffic emanating | Gleichauf discloses and/or renders obvious the system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: routing the network traffic emanating from the client device to limit network packet traversal by the client device.<br><br>*E.g.*: |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| from the client device to limit network packet traversal by the client device. | Claim 27:<br>"The method of claim 24, further comprising: receiving, by a third computer, the signal; identifying the address of the second computer such that communications from the second computer are recognized; and rejecting, by the third computer, the communications from the second computer until the infective element is removed from the second computer."<br><br>Claim 55:<br>"The software of claim 52, further operable to: receive, by a third computer, the signal; identify the address of the second computer such that communications from the second computer are recognized; and reject, by the third computer, the communications from the second computer until the infective element is removed from the second computer."<br><br>Gleichauf at [0019]:<br>"In addition, a signal may be generated and transmitted by any one of computers 16 a , 16 b , and 16 c to network management controller 14 such that a source associated with infective element 12 is identified. This signal may include an address associated with infected computer 18 , which has received infective element 12 . Based on this signal, network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions based on the protocols implemented within communication system 10 in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further."<br><br>Gleichauf at [0020]:<br>"This community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is particularly critical in network security systems where time is of the essence in containing damaging information, such as infective element 12 , once a security breach has occurred within communication system 10 . In addition, communication system 10 offers the benefit of peer monitoring, whereby only a selected number of peers within the network community need to be properly configured in order to identify a rogue within the system architecture. Network management controller 14 may respond to the identification |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | of infective element 12 with any number of appropriate remedies (as described in greater detail below) in order to prohibit infective element 12 from permeating through the system being threatened."<br><br>Gleichauf at [0032]:<br>"In accordance with a particular embodiment of the present invention, network management controller 14 may remove or reassign the IP address of infected computer 18 such that the communicating capability of infected computer 18 is disabled. Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30 . Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols. In addition, network management controller 14 may generate an alert signal to be broadcast to any element that might interact with infected computer 18 . The alert signal may include information such as: the address (or the IP address) of infected computer 18 , the type of damaging element present in the network, or remedial measures for dealing with an encounter with infected computer 18 ."<br><br>Gleichauf at [0036]:<br>"FIG. 2B is a block diagram that illustrates another example implementation network management controller 14 in which a switch 46 is coupled to network management controller 14 . Network management controller 14 may be coupled to switch 46 directly or indirectly, or alternatively switch 46 may be positioned within network management controller 14 . Switch 46 operates to receive one or more data packets from a communicating device and communicates those data packets to selected locations within communication system 10 . In addition, switch 46 may receive one or more data packets from external network 22 , policies node 38 , or any other suitable element or device within or external to communication system 10 in order to communicate information to one or more elements within communication system 10 ."<br><br>Gleichauf at [0037]:<br>"FIG. 2C is a block diagram illustrating another example implementation of network management controller 14 . A firewall 48 may be coupled to network management controller 14 and may operate |

| Claim | Exemplary Citation from Gleichauf |
|---|---|
| | to discard, delete, or otherwise avoid damaging data segments sought to be communicated to any element or device within communication system 10 . Alternatively, firewall 48 may be inclusive of network management controller 14 or coupled indirectly to network management controller 14 where appropriate. Firewall 48 is a system architecture that enforces an access control policy between two nodes, such as a virtual private network (VPN) and a public node, such as the Internet. A VPN is a private data network that makes use of the public network infrastructure. A VPN network may provide secured sharing of public sources for data by using encryption techniques to ensure that only authorized users can view or “tunnel" into a company's private networking files." |
| **[20]** The system of claim 15, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment. | Gleichauf discloses and/or renders obvious the system of claim 15, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment.<br><br>*See* [1b(a)] |

## Appendix B – Combination References

Fortinet, Inc. ("Fortinet") provides this chart subject to all reservations, objections, statements, and disclaimers set forth herein and in Fortinet's Preliminary Invalidity Contentions Cover Pleading, as well as any amendment, supplement, or modification thereof, which are incorporated herein by reference in their entirety.

On information and belief, and subject to further investigation and discovery, the following references are prior art to the '710 patent:

- U.S. Patent No. 6,832,256 to Toga ("Toga"), filed Dec. 27, 1996.
- U.S. Patent No. 6,400,996 to Hoffberg et al. ("Hoffberg '996"), issued June 4, 2002.
- U.S. Patent No. 7,966,078 to Hoffberg et al. ("Hoffberg '078"), claims priority as a continuation of Hoffberg '996.
- U.S. Patent Pub. No. 2003/0023708 to Jung ("Jung"), published January 30, 2003
- U.S. Patent No. 6,636,894 to Short et al., ("Short"), issued October 21, 2003

As illustrated in the chart below, these references disclose or render obvious certain limitations or claims of the '936 patent and can be combined with each other or other charted references for the reasons set forth in the Cover Pleading. These Preliminary Invalidity Contentions are not an admission by Fortinet that the accused products, including any current or past versions of the accused products, are covered by, or infringe the asserted claims, but are based instead on the recognition that, if the claims are interpreted to be broad enough to encompass the accused products, the claims must also be construed to have that same scope when considering whether they are invalid.

The following chart is partially based on, but is not limited by, the claim constructions implicit in Plaintiff's Infringement Contentions, to the extent that such constructions are apparent from the Infringement Contentions. Fortinet notes that in many instances, Plaintiff's Infringement Contentions fail to provide adequate notice of Plaintiff's construction of the asserted claims and fail to comply with the Court's scheduling order and other applicable rules. Fortinet does not accept the assumptions concerning the scope and meaning implicit in Plaintiff's Infringement Contentions, to the extent those assumptions are discernible, and reserves the right to challenge Plaintiff's proposed (or implied) constructions. Fortinet also reserves the right to revise and supplement these charts if and when Plaintiff is permitted to provide revised Infringement Contentions or otherwise make its positions known. To the extent that these Preliminary Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the asserted claims, Fortinet does not necessarily advocate any such construction as proper constructions of those terms or phrase. Fortinet also reserves



Netskope, Ex. 2003
Fortinet v. Netskope, IPR2026-00042

the right to revise and supplement these charts after the Court construes the claims. Citations given in the chart below are merely representative of the respective elements and are not meant to be exhaustive.

| Claim | Exemplary Citations |
|---|---|
| **[1pre]** A method of network traffic quarantine control, comprising: | |
| **[1a]** at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network; | |
| **[1b]** at the network access gateway device, performing a plurality of quarantine control functions over the client device, wherein the plurality of quarantine control functions comprises: | |
| **[1b(a)]** restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment; | |
| **[1b(b)]** restricting all network traffic emanating from the client device to an allowed network destination address to selected one or | ***E.g.*, Toga:**<br>• **2:26-42** ("A method of controlling application communications and data transfer between a first network and a second network of computers is described. Protocol exchanges, such as File Transfer Protocol (FTP) or Hypertext Transfer Protocol (HTTP), received from the first network by the second network is parsed and interpreted to determine requests within the |

| Claim | Exemplary Citations |
| --- | --- |
| more network protocols; and | application protocol. The second network of computers makes a completion decision as to whether to allow the command(s) based on the protocol information. The second network of computers may allow complete exchange or partial exchange between the application(s). The second network of computers may deny the exchange until a later time, or it may cache the exchange to allow its clients to access the data from this transfer without the need to retrieve the data a second time from the first network. Various other completion decisions based upon resource constraints, specific rights of the user are also possible.")<br>• **2:43-47** ("FIG. 1 is a block diagram of a firewall/proxy separating a first network from a second network of computers. The first network, network A, is the Internet 10 which includes the many host computers and its many HTTP, SMTP, FTP and Telnet sites, such as WEB site 12 and FTP site 13.")<br>• **2:48-55** ("Network A is coupled to Network B, which may be a corporate network of computers, for example. In one embodiment, Network B comprises a first filtering router 20, a proxy 22, and a second filtering router 24. Additionally, Network B may host a number of services such as FTP and WEB that are accessible to Network A. Network B may also host many other client computers 30 connected to its network.")<br>• **3:15-27** ("In the present invention, the proxy 22 actively monitors and interprets the protocol exchanges that occur between the Internet. The proxy looks at session information and specific commands that may be used during the protocol exchange about the content of the data, as will be described further with reference to FIG. 2. The proxy then determines completion decisions as to whether to allow the command to complete based upon the information within the protocol. The decision can be completely dynamic, based upon the current parties and environment active at that point in time. For example, the proxy may allow complete transfer or partial transfer of the data within FTP, depending on the text mode that has been set by the client.")<br>• **3:66-4:8** ("Other protocol information that can be used by the proxy to make completion decisions include specific recipients of data, auxiliary connections that might be needed or extended searching mechanisms. The proxy can access information about the users on its client systems which allows the proxy to determine whether certain users should be allowed to complete protocol transactions in particular situations. The proxy may also store information about certain destination sites and disallow certain types of accesses based upon the destination site.") |

| Claim | Exemplary Citations |
|---|---|
| | • **4:32-56** ("Some examples may help clarify possible uses of the invention. In a first example, a session is established originating from a client computer on net 30 via the proxy to a FTP site on the internet. FTP allows transfer in a text mode and in a binary mode. In one case, the proxy parses the command protocol stream to prevent a switch from one mode to the other initiated by the client computer. In another case, the proxy disallows the data being retrieved in one of the FTP modes. These restrictions may be based upon attributes of the client computer, the user of the client computer, or the FTP site. It may also be based upon the time of day or other resource constraints.<br>In a second example, a session is established via a SMTP protocol. Within the SMTP protocol, an EXPN command allows access to mailing list information. The proxy may restrict the EXPN command from being transferred between the two networks based upon predetermined rules which are stored within the proxy. Alternatively, the proxy may interpret the SMTP stream of commands to disallow email from a particular sender to be accepted for a particular recipient.<br>In a third example, a session is established between a client computer in net 30 and an internet web site via the HTTP protocol. The proxy may allow commands from the client computer to read from the web site; however, the proxy may disallow posts (or writes) to the web site.") |
| **[1c]** rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine | ***E.g.*, Short:**<br>• Abstract ("The system includes a gateway device for receiving a request from a user for access to the destination network, a user profile database comprising stored access information and in communication with the gateway device, and an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database. The AAA server determines if user is entitled to access the destination network based upon the access information stored within the user profile database, and wherein the AAA server redirects the user to a login page where the access information does not indicate the user's right to access the destination network.")<br>• 2:33-37 ("Gateway devices are typically used to provide network access to the remote portable computer user, such as users in hotels, airports and other location where the remote portable computer user may reside.") |

| Claim | Exemplary Citations |
|---|---|
| control function of the client device. | • 4:13-21 ("According to one aspect of the invention, the method can include the step of establishing a login page on a webserver local to the gateway device prior to redirecting the user to the login page. The method can also include accepting user information at the login page which is thereafter utilized by the gateway device to authorize the user access to the destination network. The user profile database can be updated with the user information.")<br>• 4:54-58 ("According to one aspect of the invention, the login page is maintained local to the gateway device. The user profile database and AAA server can also be located within the gateway device. Furthermore, the user profile database can be located within the AAA server.")<br><br>***E.g.*, Hoffberg '078 (and Hoffberg '996):**<br>• Claim 1 ("1. A router, comprising: (a) at least one IP (Internet Protocol) network interface; (b) at least one device communications interface configured to communicate with a controllable device; and (c) at least one processor configured to provide a remote control interface for controlling the processor via a markup language that is communicated using IP through at least one of said IP network interfaces, the at least one processor being configured to: (i) control data communications between said at least one of said IP network interfaces and the controllable device through said at least one device communications interface, based at least in part on processing of the markup language, (ii) monitor and analyze information contained in IP packets passing through said IP network interfaces, distinct from the markup language, and making decisions in dependence thereon, based at least in part on the processing of the markup language, and (iii) communicate control information to the controllable device through said at least one device communications interface, based at least in part on the decisions and on the processing of the markup language.")<br>• Claim 14. ("The router according to claim 1, wherein said processor is adapted to control a routing of data packets between at least two different networks.")<br>• Claim 15. ("The router according to claim 1, wherein said processor is adapted to control a network switching function.")<br>• Claim 18. ("The router according to claim 1, wherein said processor is adapted to implement network firewall functions.")<br>• Claim 22. ("The router according to claim 1, wherein said markup language comprises XML.") |

| Claim | Exemplary Citations |
|---|---|
| | • Claim 23. ("The router according to claim 1, wherein said markup language comprises HTML.")<br>• Claim 24. ("The router according to claim 1, wherein said processor is adapted to execute JAVA code.")<br>• Claim 32. ("The router of claim 1, wherein the at least one processor is further configured to provide an embedded server for interacting with a client through the at least one IP network interface using the markup language.")<br>• 147:33-39 ("With such storage, the intelligent device **3201** may also assume the standard functions of computer network servers, for example, file serving, print serving, fax serving, application serving, client/server application support, as well as traditional networking functions, such as bridging, routing, switching, virtual private network, voice-over-IP, firewall functions, remote access serving, and the like."); *see also* Hoffberg '996 at 149:52-59.<br>• 145:13-22 ("A further application of the present technologies is in a so-called "Internet appliance". These devices typically are electronic devices which have a concrete function (i.e., do more than merely act as a generic server) and typically employ at least as a secondary interface, a web browser 3205. In addition, these devices provide a TCP/IP network connection and act as a web server, usually for a limited type of data. Therefore, in addition to any real human interface on the device, a web browser 3205 may be used as a virtual interface 3304."); *see also* Hoffberg '996 at 147:33-41.<br>• 145:26-34 ("In fact, a preferred embodiment provides 3301 a rather generic device which serves as a bridge between the Internet, a public packet switched network 3202 which employs TCP/IP, and a local area network 3213, for example in a residential, industrial or office environment. The device may further abstract the interface functions for a variety of other devices 3212 as nodes on either the Internet or local area network 3213, to provide a common control system and interface."); *see also* Hoffberg '996 at 147:45-64.<br>• 146:31-34 ("Thus, since the intelligent device incorporates a web server, the physical proximity of the user is not critical for interaction with the device, and all devices on the LAN 3213 may be controlled remotely, automatically, and in synchrony."); *see also* Hoffberg '996 at 148:50-54. |
| **[2]** The method according to claim 1, wherein the action | ***E.g.*, Jung:** |

| Claim | Exemplary Citations |
|---|---|
| requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses. | • Abstract ("A system and method are provided for diagnosing, remedying and blocking harmful information including computer viruses online over a computer network via which a web server and a client are linked to each other. The method includes, on a computer network through which a web server and a client system are linked to each other, the web server receiving a connection request from the client system over the computer network. Then, the web server transmits a harmful information blocking code module to the client system. Once the transmission of the harmful information blocking code module is completed the harmful information blocking code module automatically runs on the client system to block in real time harmful information including computer viruses. The harmful information blocking code module is automatically transmitted to and installed in the client system only by online connecting to the harmful information management server, so that the harmful information detected on the client system can be actively blocked in real time without requiring a manual installation process.")<br>• [0028] ("As shown in FIG. 1A, which illustrates a system applicable to implement a preferred embodiment of the invention, a harmful information management server 110, which is a web server, has a homepage, and is linked with a client computer 130 via a computer network, such as the Internet.")<br>• [0031] ("The method begins with a homepage being constructed for online services on the harmful information management server 110 (step 210). A computer user launches a web browser on the client computer (hereinafter, referred to as merely "client") 130 (step 220). When the client 130 is connected to the harmful information management server 110 (step 240), the harmful information management server 110 transmits a harmful information blocking code module to the client 130 (step 250).")<br>• [0032] ("For this case, the connection between the client 130 and the harmful information management server 110 is accomplished by a HyperText Transfer Protocol formatted request (HTTP request), and the transferring of the harmful information blocking code module from the harmful information management server 110 to the client 130 is performed by a HTTP response. In general, the HTTP request is carried out by typing the Universal Resource Locator (URL) of the harmful information management server 110 or clicking a hyperlink associated with the URL on the web browser.")<br>• [0035] ("When the transfer of the harmful information blocking code module is completed, the harmful information blocking code module is automatically executed on the client 130 |

| Claim | Exemplary Citations |
|---|---|
| | (step 260) and blocks in real time harmful information including computer viruses (step 270). Since the harmful information blocking code module runs in real time on the client 130, unless the status displaying window is closed, the harmful information blocking code module continues to run on the client 130 even when the client 130 attempts linking to another web server. Thus, the client 130 can be provided with a harmful information blocking service for security, by a single connection to the harmful information management server 110.")<br>• [0039] ("Since the second web server 120 provide hyperlink information for use in accessing the harmful information management server 10 as well as information relating to online services to the client 130 (step 235). It is preferable that the hyperlink information is not link information for the front homepages of the harmful information management server 10, but link information that directly enables the client 130 to receive the harmful information blocking code module from the harmful information management server 110 through a separate window.")<br>• [0040] ("Since the second web server 120 provide hyperlink information for use in accessing the harmful information management server 10 as well as information relating to online services to the client 130 (step 235). It is preferable that the hyperlink information is not link information for the front homepages of the harmful information management server 10, but link information that directly enables the client 130 to receive the harmful information blocking code module from the harmful information management server 110 through a separate window.") |
| **[6]** The method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or | |

| Claim | Exemplary Citations |
|---|---|
| subordinate to the first network segment. | |
| **[7]** The method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device. | |
| **[8pre].** A computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor to perform: | |
| **[8a].** a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises: | |
| **[8b(a)]** restricting all network traffic emanating from the client device to one or more network | |

| Claim | Exemplary Citations |
|---|---|
| destination addresses that are not in or subordinate to the first network segment; | |
| **[8b(b)]** restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and | |
| **[8c].** rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to the implementation of one of the plurality of quarantine control function of the client device. | |
| **[13]** The computer program product of claim 8, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network | |

| Claim | Exemplary Citations |
|---|---|
| destination addresses in one or more network segments that are not in or subordinate to the first network segment. | |
| **[14]** The computer program product of claim 8, wherein the instructions are further translatable by the at least one processor to perform: all of the plurality of quarantine control functions over the client device. | |
| **[15pre].** A network access gateway device, comprising: | |
| **[15a].** at least one processor; and | |
| **[15b].** at least one non-transitory computer readable medium storing instructions translatable by the at least one processor to perform: | |
| **[15c].** a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, | |

| Claim | Exemplary Citations |
|---|---|
| wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises: | |
| **[15c(a)]** restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment; | |
| **[15c(b)]** restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and | |
| **[15d].** rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine | |

| Claim | Exemplary Citations |
|---|---|
| control function of the client device. | |
| **[16]** The system of claim 15, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses. | |
| **[17]** The system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: evaluating network traffic emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert. | |
| **[18]** The system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: filtering the network traffic emanating from the client device to limit network packet flow by the client device. | |

| Claim | Exemplary Citations |
|---|---|
| **[19]** The system of claim 15, wherein the instructions are further translatable by the at least one processor to perform: routing the network traffic emanating from the client device to limit network packet traversal by the client device. | |
| **[20]** The system of claim 15, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment. | |