República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 0618613-0 B1

(22) Data do Depósito: 15/11/2006

(45) Data de Concessão: 02/07/2019

(54) Título: MÉTODO E SISTEMA PARA DETECTAR UM SOFTWARE DE COMPARTILHAMENTO DE ARQUIVO PAR A PAR QUE OPERA EM UM COMPUTADOR-ALVO E SISTEMA PARA A DETECÇÃO DE UM OU MAIS APLICATIVOS DE SOFTWARE DE COMPARTILHAMENTO DE ARQUIVO PAR A PAR QUE OPERA EM UM COMPUTADOR-ALVO

(51) Int.Cl.: G06F 15/16; H04L 29/06; H04L 29/08.

(52) CPC: G06F 15/16; H04L 63/10; H04L 67/1068; H04L 67/104.

(30) Prioridade Unionista: 15/11/2005 US 60/736,794.

(73) Titular(es): KROLL INFORMATION ASSURANCE, LLC.

(72) Inventor(es): SAMUEL P. HOPKINS.

(86) Pedido PCT: PCT US2006044366 de 15/11/2006

(87) Publicação PCT: WO 2007/059224 de 24/05/2007

(85) Data do Início da Fase Nacional: 15/05/2008

(57) Resumo: MÉTODO E SISTEMA PARA DETECTAR UM SOFTWARE DE REDE PAR A PAR, SISTEMA PARA A DETECÇÃO DE UM OU MAIS APLICATIVOS DE SOFTWARE DE REDE PAR A PAR E MÉTODO E SISTEMA PARA DETECTAR UMA PARTICIPAÇÃO DE REDE PAR A PAR. A presente invenção refere-se a um sistema e método para detectar um software de rede par a par que opera em um computador-alvo. Um arquivo-alvo é criado e colocado em uma ou mais pastas no computador-alvo. Uma pesquisa é expedida em uma rede par a par para o arquivo-alvo. O software de rede par a par é detectado operando no computador-alvo de acordo com os resultados da pesquisa.

Relatório Descritivo da Patente de Invenção para **"MÉTODO E SISTEMA PARA DETECTAR UM SOFTWARE DE COMPARTILHAMENTO DE ARQUIVO PAR A PAR QUE OPERA EM UM COMPUTADOR-ALVO E SISTEMA PARA A DETECÇÃO DE UM OU MAIS APLICATIVOS DE SOFTWARE DE COMPARTILHAMENTO DE ARQUIVO PAR A PAR QUE OPERA EM UM COMPUTADOR-ALVO".**

REFERÊNCIA CRUZADA COM PEDIDOS RELACIONADOS

[001] O presente pedido reivindica a prioridade do Pedido de Patente provisório U.S. N°. 60/736 794, depositado em 15 de novembro de 2005, intitulado "System for Identifying the Presence of Peer-to-Peer Network Software Applications", e vem a ser uma continuação em parte do Pedido de Patente U.S. N°. de Série 11/103 818, depositado em 12 abril de 2005, intitulado "System for Detecting Peer-to-Peer Network Software". Ambos os pedidos acima referidos encontram-se incorporados à guisa de referência ao presente documento em suas totalidades.

CAMPO DA INVENÇÃO

[002] A presente invenção refere-se a um sistema para detectar se um sistema de computador participa ou poderia participar de uma rede par a par por meio da pesquisa de termos específicos e da detecção destes termos, ou arquivos resultantes.

ANTECEDENTES DA INVENÇÃO

[003] As redes par a pars compreendem múltiplos nós, cada nó tipicamente consistindo em um servidor de arquivo e um cliente que pode enviar e receber dados ou "mensagens de comunicação" para ou de um nó ao qual está conectado e outros nós na rede. As redes par a pars comuns e aplicativos de software são a Gnutella, o FastTrack, o Edonkey, a NeoNet, a Kazaa, a Limewire, o Morpheus, o BearShare, o Bit Torrent, a Shareaza, o Emule, e a Freenet.

[004] Em uma rede par a par, cada nó é conectado a outros nós por um meio de comunicação, tal como a Internet, diretamente ou através de algum tipo de provedor proxy. Por exemplo, quando uma solicitação de pesquisa é emitida, tal nó de origem envia uma solicitação de pesquisa para todos os nós aos quais se encontra conectado. (Vide figura 1). Estes nós pesquisam sua lista de arquivos disponíveis e caso uma correspondência for encontrada, os mesmos enviam uma resposta de volta com a localização.

[005] No entanto, uma rede de provedor proxy par a par tipicamente consiste em um nó A que é conectado a um nó B e o nó B é conectado a um nó C (vide figura 2). O nó A não é conectado ao nó C, de modo que, caso o nó A emite uma solicitação de pesquisa, a mesma será encaminhada para o nó B e o nó B pesquisará os seus arquivos disponíveis e, se uma correspondência for encontrada, o mesmo enviará uma resposta de volta para o nó A. O nó B em seguida encaminha uma solicitação do nó A para o nó C e o nó C pesquisará os arquivos disponíveis e, caso uma correspondência seja encontrada, o mesmo enviará uma resposta de volta para o nó B. O nó B em seguida encaminha esta resposta para o nó A. A figura 3 apresenta uma rede de loop de servidor não proxy, na qual cada nó é diretamente conectado a um outro.

[006] Algumas redes par a pars utilizam uma topologia de servidor proxy de nó de folha/nó de raiz (vide figura 4), na qual alguns nós são classificados como nós principais e os nós restantes são classificados como nós de folha. Os nós de folha só podem se conectar aos nós principais. Apenas os nós principais podem se conectar a outros nós principais. Quando um nó de folha emite uma solicitação de pesquisa, o mesmo envia a solicitação para o nó de raiz ao qual o mesmo se encontra conectado. O nó principal em seguida encaminha a solicitação para qualquer outro nó de folha conectado ao mesmo e ainda

para qualquer nó de raiz ao qual o mesmo se encontra conectado. Estes nós principais encaminham a solicitação para qualquer nó de folha que esteja conectado aos mesmos.

[007] Uma rede par a par é utilizada para compartilhar arquivos entre seus usuários. Os mesmos são normalmente usados para compartilhar e obter música, filmes, livros eletrônicos, e software protegidos por direito autoral, mas podem ser usados para compartilhar e adquirir quase qualquer outro tipo de arquivo. Para acessar uma rede par a par, um usuário instala um aplicativo de software de rede par a par capaz de se conectar à e utilizar a rede par a par, de maneira muito similar a um usuário que instala um navegador da rede mundial (web), como, por exemplo, o Internet Explorer, para acessar a World Wide Web (rede de alcance mundial).

[008] As organizações são colocadas em risco legal pela utilização da rede par a par por seus empregados, caso um empregado instale um aplicativo de software de rede par a par em seu PC de trabalho e utilize a rede par a par para comprar trabalhos protegidos por direito autoral. A utilização da rede par a par também consome muitas larguras de banda de rede, uma vez que os arquivos normalmente transferidos são um software grande ou arquivos de filme. Isto impõe uma carga de largura de banda sobre uma rede de computador da organização. Mesmo que seja normalmente uma violação às normas de uma corporação instalar um aplicativo de software de rede par a par, os empregados ainda assim instalam estes aplicativos.

[009] Ao instalar um aplicativo de software de rede par a par, o usuário deve selecionar uma pasta em seu sistema de computador no qual armazena qualquer arquivo transferido. Para fins de esclarecimento, uma "pasta" é usada para organizar os arquivos em um sistema de computador, também conhecida como "diretório". Todo arquivo colocado nesta pasta torna-se igualmente disponível a outros usuários.

Esta pasta é freqüentemente chamada de "Pasta Compartilhada". Por exemplo, quando um usuário n°1 (de um primeiro nó de rede) coloca um arquivo nomeado "foofile" em sua pasta compartilhada, um usuário n°2 (de um segundo nó de rede) poderia, então, acessar e baixar o arquivo. Dependendo do aplicativo de software de rede par a par usado, o usuário poderá ainda selecionar pastas adicionais a fim de torná-las disponíveis a outros usuários da rede.

[0010] Qualquer que seja o motivo, os usuários às vezes selecionam como suas pastas compartilhadas um arquivo que contém informações sensíveis ou informações que de outra forma não gostariam de compartilhar ou poderão, mais tarde, começar a colocar informações sensíveis ou informações que de outra forma não gostariam de compartilhar em suas pastas compartilhadas por engano. Geralmente, esta ação é feita por engano ou inconscientemente por parte do usuário, mas, às vezes, ela é feita por uma pessoa mal intencionada ou por um vírus. Às vezes, o aplicativo de software de rede par a par tem um bug de software que permite o compartilhamento de arquivos e pastas que o usuário jamais pensaria em compartilhar. O compartilhamento não intencional (ou malicioso) de informações pode ser maléfico ao usuário, à organização na qual trabalha, ou ainda à segurança nacional. Seria, portanto, vantajoso poder se localizar computadores com aplicativos de software de rede par a par de tal modo que os aplicativos possam ser acessados ou removidos.

[0011] Existem centenas, se não milhares, de aplicativos de software de rede par a par diferentes, cada qual tendo o seu próprio conjunto de atributos. Os métodos de detecção atuais concentram-se: 1) na identificação da presença de cada um destes diferentes aplicativos de software de rede par a par em um sistema de computador; ou 2) na colocação de um filtro incorporado baseado em hardware/software entre o sistema de computador e a Internet a fim de detectar as comunicações de rede par a

par ao procurar por seus protocolos, monitorar suas transferências, ou por um uso maior da largura de banda.

[0012] Os aplicativos de software de rede par a par são criados ou os aplicativos correntes mudam, por meio da detecção da presença de um aplicativo de software de rede par a par específico em um sistema de computador, e o monitoramento para uma comunicação de rede par a par na rede da organização se torna um desafio cada vez maior.

[0013] O método para identificar a presença de aplicativos de software de rede par a par em um sistema de computador redunda na criação de um software de cópia de projeto ("blueprint") de cada aplicativo de software de rede par a par e na verificação para checar se esta cópia de projeto existe em um sistema de computador-alvo. O software de varredura de vírus funciona da mesma maneira, no sentido de que uma cópia de projeto do vírus é criada e em seguida verificada contra cada arquivo em um sistema de computador-alvo. O uso de uma cópia de projeto de software para detectar aplicativos de software de rede par a par só é bem-sucedido quando o aplicativo de software de rede par a par é conhecido e uma cópia de projeto precisa é criada. Sempre que um novo aplicativo de software de rede par a par é criado, uma nova cópia de projeto deve ser criada e ocorre um retardo na proteção durante o desenvolvimento da cópia de projeto. Além disso, quando um aplicativo de software de rede par a par é atualizado ou modificado devido a novos desenvolvimentos, uma cópia de projeto do aplicativo de software de rede par a par não mais poderá ser válida. Isto deixa a organização exposta.

[0014] Os filtros incorporados detectam um uso de rede par a par por meio do monitoramento das comunicações de rede na rede da organização e por meio da comparação das comunicações com protocolos de rede par a par conhecidos. O uso de método de comparação de protocolo para detectar um aplicativo de software de rede par a par só

funciona quando o protocolo do aplicativo de software de rede par a par é conhecido. Toda vez que um novo aplicativo de software de rede par a par é criado, o filtro incorporado deve ser atualizado a fim de procurar o novo protocolo ou dados. Além disso, quando um aplicativo de software de rede par a par é atualizado ou modificado em função de novos desenvolvimentos, o filtro de comparação que o filtro incorporado utiliza não mais poderá ser válido. Os filtros incorporados também não funcionam nas redes par a pars nas quais a comunicação entre os usuários é criptografada. Isto deixa a organização exposta.

SUMÁRIO DA INVENÇÃO

[0015] Um aspecto da presente invenção trata de um sistema e método para detectar um software de rede par a par que opera em um computador-alvo. Um arquivo-alvo é criado, e colocado em uma ou mais pastas de um computador-alvo. Uma pesquisa é feita em uma rede par a par para o arquivo-alvo. O software de rede par a par é detectado de modo a operar no computador-alvo de acordo com os resultados da pesquisa.

[0016] Nas modalidades específicas, o arquivo-alvo pode ser colocado em uma pluralidade de pastas no computador-alvo, e, opcionalmente, contém dados que identificam unicamente o computador-alvo. Os dados podem ser criptografados e podem incluir um endereço de protocolo IP do computador-alvo, um nome do computador-alvo, um nome de um usuário do computador-alvo, e/ou um endereço de e-mail de um usuário do computador-alvo. Os dados podem ser entrados por um administrador de rede ou operador responsável pelo monitoramento do computador-alvo. O método/sistema pode ser implementado pelo menos em parte usando um software que é executado no computador-alvo, ou, de maneira alternativa, usando o software que é executado em um computador diferente do computador-alvo. Um firewall, um sistema de detecção de intrusão, um roteador, ou um aplicativo, podem

ser automaticamente notificados após a detecção do software de rede par a par no computador-alvo.

[0017] De acordo com um outro aspecto, a presente invenção trata de um sistema e método para detectar uma participação de rede par a par em um primeiro nó. Os dados de rede do primeiro nó são monitorados. Uma pesquisa é feita para um determinado termo em uma rede par a par, enquanto monitora os dados da rede. A participação par a par do primeiro nó na rede par a par é detectada quando o monitoramento identifica o termo predeterminado transmitido para o primeiro nó.

[0018] Nas modalidades específicas, um administrador responsável para monitorar o primeiro nó é notificado quando uma participação par a par é detectada. O bloqueio de acesso de dados ao primeiro nó pode ser automaticamente implementado quando uma participação par a par é detectada. Além disso, o software de rede par a par com o primeiro nó pode ser automática ou manualmente desabilitado quando uma participação par a par é detectada.

BREVE DESCRIÇÃO DOS DESENHOS

[0019] A figura 1 é uma vista esquemática simplificada de uma rede par a par de dois nós;

[0020] a figura 2 é uma vista esquemática simplificada de uma rede de servidor proxy par a par;

[0021] a figura 3 é uma vista esquemática simplificada de uma rede par a par, não proxy, de loop;

[0022] a figura 4 é uma vista esquemática simplificada de uma rede de nó de folha/nó de raiz par a par;

[0023] a figura 5 é a representação simplificada de um fluxograma de uma modalidade da presente invenção na qual um arquivo é colocado em um sistema-alvo e em seguida pesquisado via a rede par a par; e

[0024] a figura 6 é a representação simplificada de um fluxograma de uma outra modalidade da presente invenção na qual um agente de monitoramento é colocado em um sistema-alvo e em uma rede par a par. Uma pesquisa em seguida se inicia na rede par a par para ver se o agente de monitoramento detecta a pesquisa que entra na rede.

DESCRIÇÃO DAS MODALIDADES PRESENTEMENTE PREFERIDAS

[0025] Como parte da operação, os nós de uma rede par a par recebem pesquisas da rede para itens que são pesquisados por outros usuários. Quando um primeiro nó recebe uma pesquisa e tem um item de correspondência, o primeiro nó responde de volta para o nó do pesquisador. Com referência à figura 6, em uma modalidade da presente invenção, os administradores instalam um agente de monitoramento e configuram o mesmo para detectar certos termos que avançam esperados para um nó ou grupo de nós que eles desejam proteger. O agente de monitoramento pode ser um dispositivo próprio, uma peça de software, embutido em um roteador ou firewall, ou outro dispositivo de rede que passa dados de rede ou tem o potencial de monitorar dados de rede, tal como um farejador. O agente de monitoramento pode passar os dados (que são monitorados), ou pode receber uma cópia de tais dados. Os administradores em seguida expedem as pesquisas na rede par a par e vêem se os termos foram enviados para algum nó protegido. Quando o termo é detectado pelo agente de monitoramento como enviado para um nó protegido, ele sinaliza para os administradores que o nó tem um software de rede par a par. Eles teriam conhecimento disso, uma vez que o agente de monitoramento detecta a pesquisa esperada para um nó, de modo que o nó faça parte da rede par a par a receber a pesquisa. Após a detecção de que o nó tem um software de rede par a par, o agente de monitoramento é opcionalmente configurado para bloquear todas as transmissões para o

nó até que os administradores removam o software. O agente de monitoramento pode também ser configurado para notificar os administradores, após detecção, que um nó tem um software de rede par a par. O agente de monitoramento pode ser configurado para fazer uma ou outra destas funções (isto é, bloqueio/notificação) automaticamente após detecção de que um nó tem software de rede par a par.

[0026] Com referência à figura 5, uma modalidade da presente invenção vantajosamente utiliza um programa de software para criar um arquivo-alvo e coloca este arquivo-alvo nas pastas de um computador-alvo que deve ser monitorado com a finalidade de detectar se o computador-alvo contém um software de aplicativo de rede par a par. O arquivo-alvo é de preferência colocado em tantas pastas quanto possível no computador-alvo, uma vez que a "pasta compartilhada" no computador-alvo (até onde um existe) não é conhecida no aplicativo de monitoramento. Quando o computador-alvo tem um aplicativo de software de rede par a par instalado, este arquivo-alvo fica disponível para ser compartilhado com outros usuários da rede par a par, e uma pesquisa apropriada da rede par a par para o arquivo-alvo resulta na detecção do arquivo-alvo por meio de um aplicativo de monitoramento. Quando o arquivo-alvo ou seus dados é detectado em uma rede par a par, pode-se dizer que o computador-alvo está de alguma maneira participando da rede par a par e podem ser tomadas medidas no sentido de remover o aplicativo de software de rede par a par do computador-alvo. As vantagens deste sistema são que o aplicativo de monitoramento protege múltiplos computadores-alvo, tais como se encontraria em uma rede corporativa. O mesmo pode ser usado para oferecer proteção aos usuários domésticos ou consumidores contra a instalação inadvertida ou maliciosa de um aplicativo de cliente de rede par a par.

[0027] Em uma outra modalidade, um programa de software é

executado no computador-alvo. O programa de software cria um arquivo-alvo. O arquivo-alvo é colocado nas pastas no computador-alvo. Por exemplo, o arquivo-alvo é colocado em tantas pastas quanto possível, uma vez que a pasta compartilhada não é conhecida. Uma pesquisa se inicia em uma rede par a par a fim de verificar a presença do arquivo-alvo. Quando o arquivo-alvo é localizado (por exemplo, quando um nó que pesquisa o arquivo pode recuperar o mesmo), pode-se supor que o alvo de alguma forma participa da rede par a par e podem ser tomadas medidas no sentido de remover o aplicativo de software de rede par a par.

[0028] Em uma outra modalidade, um programa de software é executado no computador-alvo. O programa de software cria um arquivo-alvo. Os dados contidos neste arquivo-alvo são as informações que podem ser usadas para identificar o computador-alvo. Isto se torna útil quando há mais de um sistema de computador-alvo, e opcionalmente um nome de arquivo é usado para facilitar a pesquisa. O arquivo-alvo é colocado nas pastas do(s) computador(es)-alvo. Por exemplo, o arquivo-alvo é colocado em tantas pastas quanto possível, uma vez que não se conhece a pasta compartilhada em cada computador-alvo. Quando há mais de um sistema de computador-alvo, os dados contidos neste arquivo-alvo opcionalmente variam em cada computador-alvo. Uma pesquisa se inicia em uma rede par a par a fim de verificar a presença do arquivo-alvo. Quando o arquivo-alvo é localizado (por exemplo, quando um nó que pesquisa o arquivo pode recuperar o mesmo), o arquivo em seguida é obtido e os dados são revisados no sentido de identificar o computador-alvo correspondente.

[0029] Em uma outra modalidade, um programa de software é executado no computador-alvo. O programa de software cria um arquivo-alvo. Os dados contidos neste arquivo-alvo são as informações que podem ser usadas para identificar o computador-alvo. Isto se tor-

na útil quando há mais de um sistema de computador-alvo, e opcionalmente um nome de arquivo é usado para facilitar a pesquisa. Os dados que este arquivo-alvo inclui são criptografados a fim de proteger os conteúdos. O arquivo-alvo é colocado nas pastas do(s) computador(es)-alvo. Por exemplo, o arquivo-alvo é colocado em tantas pastas quanto possível, uma vez que não se conhece a pasta compartilhada em cada computador-alvo. Quando há mais de um sistema de computador-alvo, os dados contidos neste arquivo-alvo opcionalmente variam em cada computador-alvo. Uma pesquisa se inicia em uma rede par a par a fim de verificar a presença do arquivo-alvo. Quando o arquivo-alvo é localizado (por exemplo, quando um nó que pesquisa o arquivo pode recuperar o mesmo), o arquivo é em seguida obtido. Quando o arquivo é obtido, os dados contidos no mesmo são decriptografados e revisados a fim de identificar o computador-alvo correspondente.

[0030] Em uma outra modalidade, um programa de software é executado em um sistema de computador que tem acesso aos sistemas de arquivo de um sistema-alvo. O programa de software cria um arquivo-alvo. O arquivo-alvo é colocado nas pastas dos computadores-alvo (isto é, no computador que deve ser monitorado com a finalidade de detectar se o computador-alvo contém o software de aplicação de rede par a par). Por exemplo, o arquivo-alvo é colocado em tantas pastas quanto possível, uma vez que a pasta compartilhada não é conhecida. Uma pesquisa se inicia em uma rede par a par a fim de verificar a presença do arquivo-alvo. Quando o arquivo-alvo é localizado (por exemplo, quando um nó que pesquisa o arquivo pode recuperar o mesmo), pode-se supor que o computador-alvo de alguma forma participa da rede par a par e medidas podem ser tomadas no sentido de remover o aplicativo de software de rede par a par do computador-alvo.

[0031] Em uma outra modalidade, um arquivo-alvo é colocado nas

pastas dos computadores-alvo. O arquivo-alvo é colocado em tantas pastas quanto possível, uma vez que a pasta compartilhada não é conhecida. Uma pesquisa se inicia em uma rede par a par a fim de verificar a presença do arquivo-alvo. Quando o arquivo-alvo é localizado (por exemplo, quando um nó que pesquisa o arquivo pode recuperar o mesmo), pode-se supor que o alvo de alguma forma participa da rede par a par e medidas podem ser tomadas no sentido de remover o aplicativo de software de rede par a par do computador-alvo.

[0032] Em uma outra modalidade, um programa de software é executado em um sistema de computador que tem acesso a um ou mais sistemas de arquivo do sistema-alvo. O programa de software cria um arquivo-alvo. Os dados contidos neste arquivo-alvo são informações que podem ser usadas para identificar o(s) computador(es)-alvo. Isto se torna útil quando há mais de um sistema de computador-alvo, e opcionalmente um nome de arquivo é usado para facilitar a pesquisa. O arquivo-alvo é colocado nas pastas do(s) computador(es)-alvo. Por exemplo, o arquivo-alvo é colocado em tantas pastas quanto possível, uma vez que a pasta compartilhada de cada computador-alvo não é conhecida. Quando há mais de um sistema de computador-alvo, os dados contidos no arquivo-alvo opcionalmente variam em cada computador-alvo. Uma pesquisa se inicia em uma rede par a par a fim de verificar a presença do arquivo-alvo. Quando o arquivo-alvo é localizado, o arquivo em seguida é obtido e os dados são revisados no sentido de identificar o computador-alvo correspondente.

[0033] Em uma outra modalidade, um programa de software é executado em um sistema de computador que tem acesso a um ou mais sistemas de arquivo dos sistemas-alvo. O programa de software cria um arquivo-alvo. Os dados contidos neste arquivo-alvo são as informações que podem ser usadas para identificar o(s) computador(es)-alvo. Isto se torna útil quando há mais de um sistema de computador-

alvo, e opcionalmente um nome de arquivo é usado para facilitar a pesquisa. Os dados que este arquivo-alvo inclui são criptografados a fim de proteger os conteúdos. O arquivo-alvo é colocado nas pastas do(s) computador(es)-alvo. Por exemplo, o arquivo-alvo é colocado em tantas pastas quanto possível, uma vez que a pasta compartilhada em cada computador-alvo não é conhecida. Quando há mais de um sistema de computador-alvo, os dados contidos neste arquivo-alvo opcionalmente variam em cada computador-alvo. Uma pesquisa se inicia em uma rede par a par a fim de verificar a presença do arquivo-alvo. Quando o arquivo-alvo é localizado, o arquivo é em seguida obtido. Quando o arquivo é obtido, os dados contidos no mesmo são decriptografados e revisados a fim de identificar o computador-alvo correspondente.

[0034] Em ainda uma outra modalidade, um arquivo-alvo é colocado em um sistema-alvo e uma pesquisa é iniciada via a rede par a par para o arquivo-alvo. Quando o arquivo é detectado, ocorre uma notificação. Por exemplo, um administrador responsável pelo monitoramento do computador-alvo recebe uma comunicação eletrônica informando que o computador-alvo opera um aplicativo de software de rede par a par.

[0035] Em ainda uma outra modalidade, um arquivo-alvo é colocado em um sistema-alvo. Um agente de monitoramento é colocado entre o sistema-alvo e a rede par a par. Uma pesquisa se inicia via a rede par a par para o arquivo-alvo. Quando o arquivo é detectado pelo agente de monitoramento, ocorre, em seguida, uma notificação. Por exemplo, um administrador responsável pelo monitoramento do computador-alvo recebe uma comunicação eletrônica informando que o computador-alvo opera um aplicativo de software de rede par a par. Opcionalmente, o agente de monitoramento automaticamente desabilita o acesso ao nó que tem o software de rede par a par (isto é, o sis-

tema-alvo).

[0036] Em ainda uma outra modalidade, um agente de monitoramento é colocado entre o sistema-alvo e a rede par a par. Uma pesquisa é iniciada para um termo específico via a rede par a par. O agente de monitoramento é configurado para monitorar os dados esperados nos nós e é configurado para proteger (por exemplo, o sistema-alvo). Quando o agente de monitoramento detecta o termo específico, o mesmo pressupõe que o sistema-alvo tem o software de rede par a par, e automaticamente desabilita o acesso ao sistema-alvo.

[0037] Em ainda um outra modalidade, um agente de monitoramento é colocado entre o computador-alvo e a rede par a par. Este agente de monitoramento pode ser um dispositivo próprio embutido em um roteador ou firewall, ou outro dispositivo de rede que passa dados de rede. Um programa de software é executado no computador-alvo. O programa de software cria um arquivo-alvo. O arquivo-alvo é colocado nas pastas dos computadores-alvo. Por exemplo, o arquivo-alvo é colocado em tantas pastas quanto possível, uma vez que a pasta compartilhada não é conhecida. Uma pesquisa é iniciada em uma rede par a par a fim de verificar a presença do arquivo-alvo. Quando o agente de monitoramento detecta a cadeia da pesquisa para o arquivo, o agente de monitoramento automaticamente bloqueia o tráfego para o e do computador-alvo a fim de impedir o acesso à rede.

[0038] Em ainda uma outra modalidade, um agente de monitoramento é colocado entre o computador-alvo e a rede par a par. Este agente de monitoramento pode ser um dispositivo próprio embutido em um roteador ou firewall, ou outro dispositivo de rede que passa dados de rede. Um programa de software é executado em um ou mais computadores-alvo. O programa de software cria um arquivo-alvo. Os dados contidos neste arquivo-alvo são informações que podem ser usadas para identificar o computador-alvo. Isto é útil quando há mais de um sis-

tema de computador-alvo, e opcionalmente um nome de arquivo é usado para facilitar a pesquisa. Os dados que este arquivo-alvo inclui são criptografados a fim de proteger os conteúdos. O arquivo-alvo é colocado nas pastas do(s) computador(es)-alvo. Por exemplo, o arquivo-alvo é colocado em tantas pastas quanto possível, uma vez que a pasta compartilhada não é conhecida. Quando há mais de um sistema de computador-alvo, os dados contidos neste arquivo-alvo opcionalmente variam para cada computador-alvo. Uma pesquisa é iniciada em uma rede par a par a fim de verificar a presença do arquivo-alvo. Quando o arquivo-alvo é localizado, o arquivo é em seguida obtido. Quando o arquivo é obtido, os dados contidos no mesmo são decriptografados e revisados a fim de identificar o computador-alvo correspondente. O sistema de pesquisa em seguida notifica o agente de monitoramento, que automaticamente bloqueia o tráfego para o e do(s) computador(es)-alvo identificado a fim de impedir o acesso à rede.

[0039] Em ainda uma outra modalidade, uma rede corporativa é protegida ao se colocar um arquivo-alvo nas pastas dos computadores localizados na rede, opcionalmente trocando o nome de cada arquivo, ou opcionalmente criptografando os dados contidos no mesmo. O(s) arquivo(s) é(são) pesquisados para uma rede par a par, e, quando o arquivo é detectado, o mesmo é opcionalmente transferido. Os administradores ou o usuário podem em seguida ser notificados.

[0040] Em uma modalidade, a presente invenção é implementada em um sistema de computador que contém uma unidade de processador, uma memória principal, e um barramento de interconexão. A unidade de processador pode conter um único microprocessador, ou pode conter uma pluralidade de microprocessadores para a configuração do computador como um sistema multiprocessador. A memória principal armazena, em parte, instruções e dados para execução por parte da unidade de processador. Quando a capacidade do sistema da pre-

sente invenção é total ou parcialmente implementado em um software, a memória principal pode ser usada para armazenar o código executável quando em operação. A memória principal pode incluir bancos de memória de acesso aleatório dinâmico, assim como uma memória de alta velocidade.

[0041] O sistema de computador pode incluir ainda um dispositivo de memória de massa, dispositivos periféricos, unidades de meio de memória portátil, um dispositivo de controle de entrada, um sub-sistema gráfico, e um vídeo de saída. O sistema de computador pode ser conectado através de um ou mais meios de transporte de dados. Por exemplo, a unidade de processador e a memória principal podem ser conectadas via um barramento de microprocessador local, e o dispositivo de memória de massa, os dispositivos periféricos, as unidades de meio de memória portátil, o sub-sistema gráfico podem ser conectados via um ou mais barramentos de entrada/saída (I/O). O dispositivo de memória de massa, que pode ser implementado com uma unidade de disco magnético ou com uma unidade de disco ótico, é um dispositivo de memória não volátil para o armazenamento de dados e instruções para uso pela unidade de processador. Em uma modalidade de software, o dispositivo de memória de massa armazena o software para carregamento para a memória principal.

[0042] O(s) dispositivo(s) de controle de entrada provê uma porção da interface de usuário para um usuário do sistema de computador. Os dispositivos de controle de entrada podem incluir um teclado alfanumérico para a entrada de informações alfanuméricas ou outras informações de teclas, um dispositivo de controle de cursor, como, por exemplo, um mouse, um trackball, uma caneta, ou teclas de direção de cursor. A fim de exibir informações textuais e gráficas, o sistema de computador contém o sub-sistema gráfico e o vídeo de saída. O vídeo de saída pode incluir um vídeo de tubo de raios catódicos ou um vídeo de

cristal líquido. O sub-sistema gráfico recebe informações textuais ou gráficas e processa as informações para saída para o vídeo de saída.

[0043] Os componentes contidos no sistema de computador são os tipicamente encontrados nos sistemas de computador de uso geral, e, com efeito, estes componentes pretendem representar uma ampla categoria de tais componentes de computador bem-conhecidos na técnica.

[0044] O sistema pode ser implementado em um hardware ou em um software. Para algumas modalidades de software, o software inclui uma pluralidade de instruções executáveis em computador para implementação em um sistema de computador de uso geral. Antes de carregar em um sistema de computador de uso geral, o sistema pode residir como informação codificada em um meio legível em computador, como, por exemplo, como um disco flexível magnético, um disco compacto de fita magnética ou um disco compacto de memória de leitura (CD-ROM). Em uma modalidade de hardware, o sistema pode compreender um processador dedicado incluindo instruções de processador para a execução das funções descritas no presente documento. Podem também ser desenvolvidos circuitos no sentido de realizar as funções descritas no presente documento.

Exemplos

[0045] Os exemplos a seguir ilustram as várias modalidades de sistemas de acordo com a presente invenção.

Exemplo 1:

[0046] Este exemplo ilustra um sistema para a detecção de aplicativos de software de rede par a par por meio da criação de um arquivo-alvo específico, colocando este arquivo-alvo nas pastas de um computador-alvo, e pesquisando este arquivo-alvo em uma rede par a par.

[0047] Neste exemplo, um usuário instalou um aplicativo de software de rede par a par em um sistema de computador n°1. Um adminis-

trador de rede quer identificar se este sistema de computador tem um aplicativo de software de rede par a par instalado. O administrador de rede executa o software de detecção. O software de detecção cria um arquivo nomeado "123456.txt" e coloca este arquivo em cada pasta do sistema de computador n°1. O administrador de rede em seguida expede uma pesquisa em uma rede par a par para o arquivo "123456.txt". O administrador de rede localiza um arquivo nomeado "123456.txt". O administrador de rede agora sabe que o sistema de computador n°1 tem um aplicativo de software de rede par a par instalado.

Exemplo 2:

[0048] Este exemplo ilustra um sistema para a detecção de aplicativos de software de rede par a par por meio da criação de um arquivo-alvo específico, da colocação deste arquivo-alvo nas pastas de um computador-alvo, e da pesquisa deste arquivo-alvo em uma rede par a par.

[0049] Neste exemplo, um usuário instalou um aplicativo de software de rede par a par em um sistema de computador n°1 que tem um endereço de IP de 192.168.0.1. Um administrador de rede quer identificar se este sistema de computador tem um aplicativo de software de rede par a par instalado no mesmo. O administrador de rede executa o software de detecção. O software de detecção cria um arquivo nomeado "123456.txt", com os conteúdos deste arquivo sendo o endereço de protocolo IP do sistema de computador n°1. O software de detecção coloca este arquivo em cada pasta do sistema de computador n°1. O administrador de rede em seguida expede uma pesquisa em uma rede par a par para o arquivo "123456.txt". O administrador de rede localiza um arquivo nomeado "123456.txt". O administrador de rede obtém o arquivo e revisa os dados. O endereço de protocolo IP dentro do arquivo é "192.168.0.1". O administrador de rede agora sabe que o sistema de computador n°1 tem um aplicativo de software de rede par a par instalado no mesmo.

Exemplo 3:

[0050] Este exemplo ilustra um sistema para a detecção de um aplicativo de software de rede par a par em múltiplos sistemas de computador por meio da criação de um arquivo-alvo específico, da colocação deste arquivo-alvo nas pastas de um computador-alvo, e da pesquisa deste arquivo-alvo em uma rede par a par.

[0051] Neste exemplo, há cinco sistemas de computador em uma rede:

[0052] O sistema de computador n°1 com um endereço de protocolo IP de 192.168.0.1

[0053] O sistema de computador n°2 com um endereço de protocolo IP de 192.168.0.2

[0054] O sistema de computador n°3 com um endereço de protocolo IP de 192.168.0.3

[0055] O sistema de computador n°4 com um endereço de protocolo IP de 192.168.0.4

[0056] O sistema de computador n°5 com um endereço de protocolo IP de 192.168.0.5

[0057] O administrador de rede quer identificar se algum destes sistemas de computador tem um aplicativo de software de rede par a par instalado nos mesmos. Um ou mais usuários instalam um aplicativo de software de rede par a par no sistema de computador n°1 e no sistema de computador n°3. O administrador de rede executa o software de detecção em cada sistema de computador. O software de detecção em cada sistema de computador cria um arquivo nomeado "123456.txt", com os conteúdos deste arquivo sendo o endereço de protocolo IP do sistema de computador correspondente. O software de detecção coloca este arquivo em cada pasta do sistema de computador correspondente. O administrador de rede então lança uma pesquisa sobre uma rede par a par para "123456.txt". O administrador de re-

de localiza dois arquivos nomeados "123456.txt". O administrador de rede obtém estes arquivos e revisa os dados. O endereço de protocolo IP dentro do arquivo n°1 é "192.168.0.1" e o endereço de protocolo IP dentro do arquivo n°2 é "192.168.0.3". O administrador de rede agora sabe que o sistema de computador n°1 e o sistema de computador n°3 possuem um aplicativo de software de rede par a par instalado nos mesmos.

Exemplo 4:

[0058] Este exemplo ilustra um sistema para a detecção de um aplicativo de software de rede par a par nos computadores de uma rede que compartilham os mesmos endereços de protocolo IP por meio da criação de um arquivo-alvo específico, da colocação deste arquivo-alvo nas pastas de um computador-alvo, e da pesquisa deste arquivo-alvo em uma rede par a par.

[0059] Neste exemplo há uma rede corporativa que inclui dois escritórios remotos. Cada rede de escritório remoto tem dois sistemas de computador. Cada sistema de computador tem um único nome de computador. Cada escritório remoto utiliza um esquema de protocolo IP que é igual ao outro. Os endereços de protocolo IP resultantes são:

[0060] Escritório Remoto n°1, Sistema de Computador n°1: COMPA, 192.168.0.1

[0061] Escritório Remoto n°1, Sistema de Computador n°2: COMPB, 192.168.0.2

[0062] Escritório Remoto n°2, Sistema de Computador n°1: COMPB, 192.168.0.1

[0063] Escritório Remoto n°2, Sistema de Computador n°2: COMPD, 192.168.0.2

[0064] Um ou mais usuários instalaram um aplicativo de software de rede par a par no sistema de computador n°1 do escritório remoto n°1 e no sistema de computador n°2 do escritório remoto n°2. Um ad-

ministrador de rede quer identificar se algum sistema de computador na rede de escritório remoto tem um aplicativo de software de rede par a par instalado no mesmo. O administrador de rede executa o software de detecção em todos os sistemas de computador em ambas as redes de escritório remoto. O software de detecção em cada sistema de computador cria um arquivo nomeado "123456.txt", com os conteúdos deste arquivo sendo o endereço de protocolo IP e o nome do sistema de computador correspondente. O software de detecção coloca este arquivo em cada pasta do sistema de computador correspondente. O administrador de rede em seguida expede uma pesquisa em uma rede par a par para "123456.txt". O administrador de rede localiza dois arquivos nomeados "123456.txt". O administrador de rede obtém estes arquivos e revisa os dados. O endereço de protocolo IP dentro do arquivo n°1 é "192.168.0.1" e o endereço de protocolo IP dentro do arquivo n°2 é "192.168.0.2". O nome do arquivo n°1 é "COMPA" e o nome do arquivo n°2 é "COMPD". O administrador de rede agora sabe que o sistema de computador n°1 no escritório remoto n°1 e o sistema de computador n°2 no escritório remoto n°2 têm um aplicativo de software de rede par a par instalado no mesmo.

Exemplo 5:

[0065] Este exemplo ilustra um sistema de segurança para a detecção de um aplicativo de software de rede par a par em múltiplos sistemas de computador por meio da criação de um arquivo-alvo específico com dados específicos, a criptografia destes dados, a colocação deste arquivo nas pastas de um computador-alvo, e da pesquisa deste arquivo em uma rede par a par.

[0066] Neste exemplo, há cinco sistemas de computador em uma rede:

[0067] O sistema de computador n°1 com um endereço de protocolo IP de 192.168.0.1

[0068] O sistema de computador n°2 com um endereço de protocolo IP de 192.168.0.2

[0069] O sistema de computador n°3 com um endereço de protocolo IP de 192.168.0.3

[0070] O sistema de computador n°4 com um endereço de protocolo IP de 192.168.0.4

[0071] O sistema de computador n°5 com um endereço de protocolo IP de 192.168.0.5

[0072] O administrador de rede quer identificar de uma maneira segura se algum destes sistemas de computador possui um aplicativo de software de rede par a par instalado no mesmo. Um ou mais usuários instalaram um aplicativo de software de rede par a par no sistema de computador n°1 e no sistema de computador n°3. O administrador de rede executa o software de detecção em cada sistema de computador. O software de detecção em cada sistema de computador cria um arquivo nomeado "123456.txt", com os conteúdos deste arquivo sendo o endereço de protocolo IP do sistema de computador correspondente. O software de detecção criptografa os conteúdos do arquivo. O software de detecção coloca este arquivo em cada pasta do sistema de computador correspondente. O administrador de rede em seguida expede uma pesquisa em uma rede par a par para o arquivo "123456.txt". O administrador de rede localiza dois arquivos nomeados "123456.txt". O administrador de rede obtém estes arquivos, decriptografa os dados, e revisa os dados. O endereço de protocolo IP dentro do arquivo n°1 é "192.168.0.1" e o endereço de protocolo IP dentro do arquivo n°2 é "192.168.0.3". O administrador de rede agora sabe que o sistema de computador n°1 e o sistema de computador n°3 têm um aplicativo de software de rede par a par instalado nos mesmos.

[0073] Finalmente, será apreciado pelos versados na técnica que mudanças podem ser feitas às modalidades descritas acima sem se

afastar do amplo conceito da presente invenção. Entenda-se, portanto, que a presente invenção não se limita às modalidades particulares apresentadas, mas, sim, pretende cobrir modificações dentro do espírito e âmbito da presente invenção conforme definida nas reivindicações em apenso.

REIVINDICAÇÕES

1. Método para detectar um software de compartilhamento de arquivo par a par que opera em um computador-alvo, caracterizado por compreender as etapas de:

a) criar um arquivo-alvo, e colocar o dito arquivo-alvo em uma ou mais pastas do computador-alvo, em que o arquivo-alvo contém dados que identificam unicamente o computador-alvo;

b) expedir uma pesquisa em uma rede de compartilhamento de arquivo par a par para o dito arquivo-alvo; e

c) se o arquivo-alvo está localizado em uma rede de compartilhamento de arquivo par a par como resultado da pesquisa, detectar que o software de compartilhamento de arquivo par a par está operando no computador-alvo de acordo com os resultados da pesquisa, e impedir que o computador-alvo participe na rede de compartilhamento de arquivo par a par bloqueando o acesso de dados para o computador-alvo.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o arquivo-alvo é colocado em uma pluralidade de pastas do dito computador-alvo.

3. Método de acordo com a reivindicação 1, caracterizado pelo fato de que os ditos dados são criptografados.

4. Método de acordo com a reivindicação 1, caracterizado pelo fato de que os ditos dados incluem um endereço de protocolo IP do computador-alvo.

5. Método de acordo com a reivindicação 1, caracterizado pelo fato de que os ditos dados contêm um nome do computador-alvo.

6. Método de acordo com a reivindicação 1, caracterizado pelo fato de que os ditos dados contêm um nome de um usuário do computador-alvo.

7. Método de acordo com a reivindicação 1, caracterizado

pelo fato de que os ditos dados contêm um endereço de e-mail de um usuário do computador-alvo.

8. Método de acordo com a reivindicação 1, caracterizado pelo fato de que os ditos dados contêm informações inseridas por um administrador de rede ou operador responsável pelo monitoramento do computador-alvo.

9. Método de acordo com a reivindicação 1, caracterizado por compreender ainda a etapa de:

notificar pelo menos um dentre um firewall, um sistema de detecção de intrusão, um roteador, ou um aplicativo que um software de rede par a par foi detectado, em que a notificação é feita baseada de acordo com uma saída da etapa de detectar.

10. Sistema para detectar um software de compartilhamento de arquivo par a par que opera em um computador-alvo, caracterizado por compreender:

um meio de memória para armazenar instruções; e

um dispositivo de entrada de usuário para o recebimento da entrada de usuário; e

uma unidade de processador operável para processar a dita entrada de usuário e utilizar as ditas instruções para:

criar um arquivo-alvo, em que o arquivo-alvo contém dados que identificam unicamente o computador-alvo;

colocar o dito arquivo-alvo em uma ou mais pastas no computador-alvo;

expedir uma pesquisa em uma rede de compartilhamento de arquivos par a par para o dito arquivo-alvo; e

se o arquivo-alovo é localizado como um resultado da pesquisa, detectar que software de compartilhamento de arquivo par a par está operando no computador-alvo de acordo com os resultados da pesquisa, e impedir que o computador-alvo participe na rede de com-

partilhamento de arquivo par a par bloqueando o acesso de dados ao computador-alvo.

11. Sistema de acordo com a reivindicação 10, caracterizado pelo fato de que a unidade de processador é operável no sentido de processar a dita entrada de usuário e utilizar as ditas instruções para colocar o arquivo-alvo em uma pluralidade de pastas no computador-alvo.

12. Sistema de acordo com a reivindicação 10, caracterizado pelo fato de que os ditos dados são criptografados.

13. Sistema de acordo com a reivindicação 10, caracterizado pelo fato de que os ditos dados incluem um endereço de protocolo IP do computador-alvo.

14. Sistema de acordo com a reivindicação 10, caracterizado pelo fato de que os ditos dados contêm um nome do computador-alvo.

15. Sistema de acordo com a reivindicação 10, caracterizado pelo fato de que os ditos dados contêm um nome de um usuário do computador-alvo.

16. Sistema de acordo com a reivindicação 10, caracterizado pelo fato de que os ditos dados contêm um endereço de e-mail de um usuário do computador-alvo.

17. Sistema de acordo com a reivindicação 10, caracterizado pelo fato de que os ditos dados contêm informações entradas por um operador ou administrador de rede responsável pelo monitoramento do computador-alvo.

18. Sistema de acordo com a reivindicação 10, caracterizado pelo fato de que a unidade de processador notifica automaticamente pelo menos um dentre um firewall, um sistema de detecção de intrusão, um roteador, ou um aplicativo, após a detecção de um software de rede par a par.

19. Sistema para a detecção de um ou mais aplicativos de software de compartilhamento de arquivo par a par que opera em um computador-alvo, caracterizado por compreender:

a) um meio para criar um arquivo-alvo, e colocar o dito arquivo-alvo em uma ou mais pastas dos computadores-alvo, em que o arquivo-alvo contém dados que identificam unicamente o computador-alvo;

b) um meio para expedir uma pesquisa em uma rede de compartilhamento de arquivo par a par para o dito arquivo-alvo;

c) um meio para detectar que o software de compartilhamento de arquivo par a par está operando no computador-alvo de acordo com os resultados da pesquisa, e impedir que o computador-alvo participe na rede de compartilhamento de arquivo par a par bloqueando o acesso de dados para o primeiro nó.

20. Sistema de acordo com a reivindicação 19, caracterizado pelo fato de que o arquivo-alvo é colocado em uma pluralidade de pastas dos computadores-alvo.

21. Sistema de acordo com a reivindicação 19, caracterizado pelo fato de que o arquivo-alvo contém dados que identificam unicamente o computador-alvo.

Fig 1

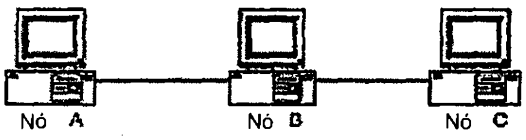

Fig 2

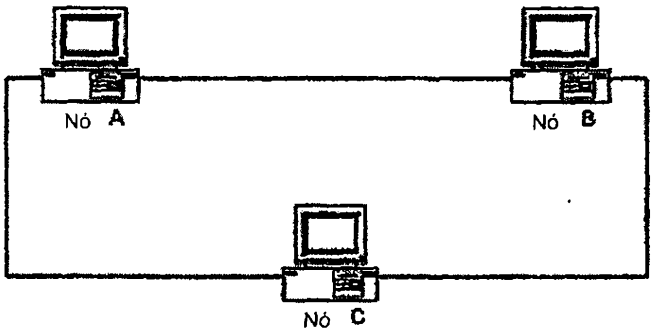

Fig 3

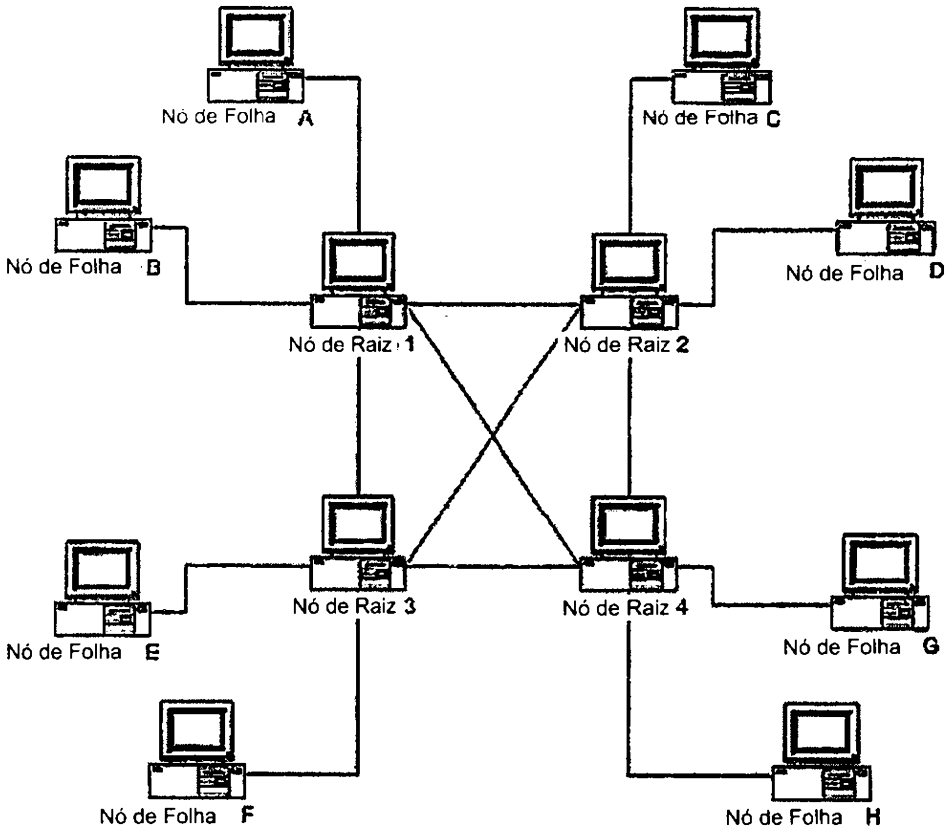
Nó de Folha A
Nó de Folha C
Nó de Folha B
Nó de Folha D
Nó de Raiz 1
Nó de Raiz 2
Nó de Raiz 3
Nó de Raiz 4
Nó de Folha E
Nó de Folha G
Nó de Folha F
Nó de Folha H

Fig 4

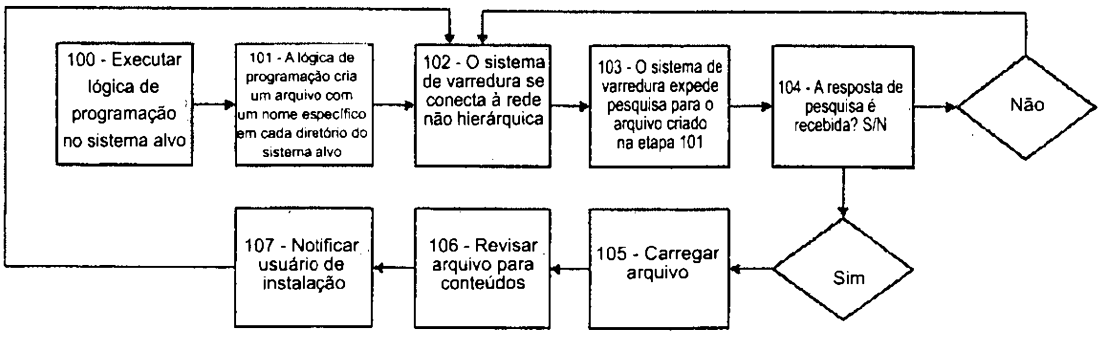
100 - Executar lógica de programação no sistema alvo
101 - A lógica de programação cria um arquivo com um nome específico em cada diretório do sistema alvo
102 - O sistema de varredura se conecta à rede não hierárquica
103 - O sistema de varredura expede pesquisa para o arquivo criado na etapa 101
104 - A resposta de pesquisa é recebida? S/N
Não
Sim
105 - Carregar arquivo
106 - Revisar arquivo para conteúdos
107 - Notificar usuário de instalação

FIG 5

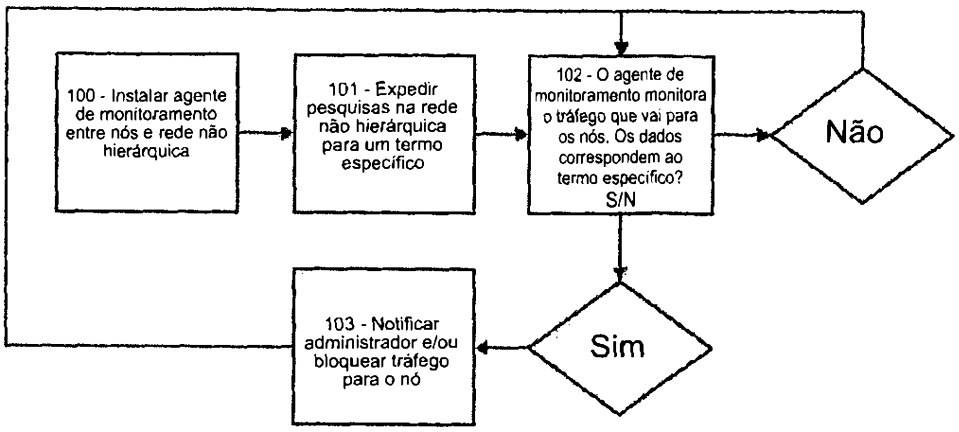
100 - Instalar agente de monitoramento entre nós e rede não hierárquica
101 - Expedir pesquisas na rede não hierárquica para um termo específico
102 - O agente de monitoramento monitora o tráfego que vai para os nós. Os dados correspondem ao termo específico? S/N
Não
Sim
103 - Notificar administrador e/ou bloquear tráfego para o nó

FIG 6