(11) Número de Publicação: **PT 1299791 E**

(51) Classificação Internacional:
G06F 1/00 (2006.01)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2001.07.06**

(30) Prioridade(s): **2000.07.07 GB 0016835**

(43) Data de publicação do pedido: **2003.04.09**

(45) Data e BPI da concessão: **2007.05.02**
059/2007

(73) Titular(es):
MESSAGELABS LIMITED
1270 LANSDOWNE COURT GLOUCESTER BUSINESS PARK GLOUCESTER GL3 4AB GB

(72) Inventor(es):
ALEXANDER SHIPP GB

(74) Mandatário:
FERNANDO ANTÓNIO FERREIRA MAGNO
R DAS FLORES 74 4 AND LISBOA PT

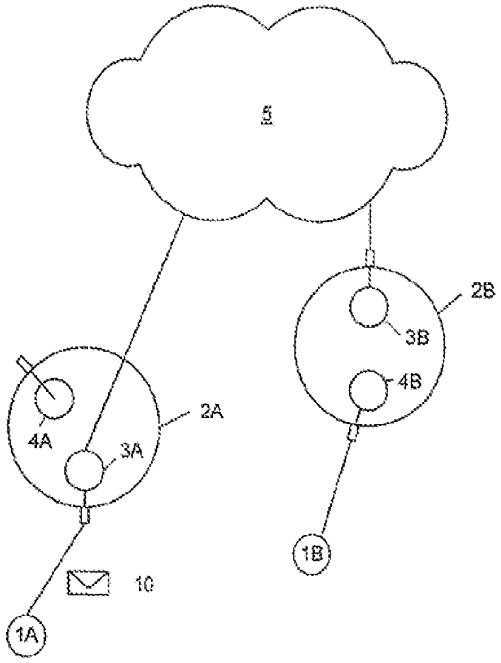
(54) Epígrafe: **MÉTODO E SISTEMA PARA PROCESSAMENTO DE CORREIO ELÉCTRONICO**

(57) Resumo:

RESUMO

"Método e sistema para processamento de correio electrónico"

Um sistema para processamento de mensagens de correio electrónico integra meios para lidar com vírus previamente desconhecidos. O sistema monitoriza padrões de tráfego de correio electrónico para identificar padrões característicos de um ataque de vírus e toma acção correctiva quando é detectado um ataque. As mensagens de correio electrónico individuais são analisadas e, se qualquer uma das partes constituintes contiver conteúdos, nos quais seja possível conter um vírus, os dados característicos derivados da mensagem de correio electrónico são registados numa base de dados que é analisada para padrões de tráfego que indiquem ataque.



DESCRIÇÃO

"Método e sistema para processamento de correio electrónico"

INTRODUÇÃO

O presente invento refere-se a um método e sistema para, processar correio electrónico em particular para detectar ataques de vírus. O invento é particularmente, mas não em exclusivo, aplicável ao processamento de correio electrónico por ISP (fornecedores de serviço de Internet)

ANTECEDENTES DO INVENTO

Deverá ser salientado que algumas explicações de suporte lógico maléfico utilizam o termo "vírus" num estrito senso como relativo a suporte lógico com características particulares em termos de propagação, possivelmente também multiplicação, e efeito que são distintas das outras formas tais como "trojan horses" (cavalos de Tróia), "worms" (vermes), etc. No entanto, neste fascículo, incluindo as reivindicações em anexo, o termo vírus é utilizado no sentido geral de qualquer suporte lógico que por intenção criminosa (ou acidente) provoque efeitos indesejados.

Verificadores de vírus convencionais encontram vírus por pesquisa de padrões conhecidos em ficheiros, por verificação de ficheiros novos ou alterados num sistema de ficheiros ou por execução de programas suspeitos num ambiente emulador de área de teste para detectar actividade do tipo vírus.

A utilização crescente de correio electrónico, tanto através da Internet como em redes privadas, aumenta a exposição de utilizadores finais individuais e operações para disrupção maléfica. Recentemente têm ocorrido ataques de vírus com origem em correio electrónico que se disseminam pelo mundo numa questão de horas. Algum grau de protecção pode ser conseguido por análise das mensagens de correio electrónico e dos seus anexos para vírus e obviamente isto é melhor realizado numa base centralizada, por exemplo, por ISP e outros que operem portas de interligação de correio electrónico, em vez de deixá-lo para os utilizadores finais

que podem ter ou não os recursos, o conhecimento ou a inclinação para tomarem as suas próprias medidas anti-vírus.

No entanto, mesmo com análise centralizada subsiste ainda um problema com vírus novos. Deixando de parte a questão de como um vírus novo é detectado primeiro, se por medidas tomadas por um ISP ou semelhante, ou numa máquina do utilizador final, os passos necessários para mitigar o efeito de um ataque do mesmo levam tempo para colocar em efeito, e na altura em que os mesmos ocorrerem, os piores efeitos do ataque podem já ter ocorrido, por todo o mundo. Estes passos tipicamente incluem a identificação de uma cadeia característica de bytes ou outra "assinatura" que identifique o vírus, a disseminação desta informação para os sítios de análise de vírus e a programação dos dispositivos de análise com esta informação, leva tempo, e entretanto o ataque está livre de se disseminar. Isto tornou-se particularmente problemático recentemente com o tipo de vírus que pode efectivamente auto multiplicar-se por criação e envio de cópias da mensagem de correio electrónico que contenham o mesmo, por exemplo, por acesso a um livro de endereços de correio electrónico (por exemplo o disponível a um cliente de correio electrónico do utilizador final) e então utilizar serviços disponíveis na máquina para enviar uma cópia da mensagem de correio electrónico para o próprio ou qualquer dos endereços encontrados. Esta táctica pode propagar-se entre continentes numa questão de minutos e resultar numa "explosão" geométrica do número de instâncias do mesmo.

TÉCNICA ANTERIOR

US-A-5832208 (Chem): é um exemplo de um sistema cliente/servidor anterior com uma facilidade no servidor que analisa vírus em anexos de mensagens de correio electrónico antes de fazer a entrega.

WO 93/2272 (MuliInform): refere-se a um monitor de rede que remonta pacotes de rede em ficheiros que são então analisados para vírus com a utilização de uma técnica baseada em assinatura.

WO 00/05650 & WO 00/05852 (Raytheon): refere-se a um "sistema de análise de segurança de informação" que inclui, entre outros, meios para registo de tráfego de correio electrónico e uma facilidade para examinar a funcionalidade de código suspeito para determinar se está presente um vírus de computador.

OBJECTO DO INVENTO

O presente invento procura proporcionar um método e sistema para processamento de correio electrónico que possa detectar a disseminação de um vírus previamente desconhecido, criado por correio electrónico e deste modo mitigar os efeitos de um ataque de um vírus deste tipo.

SUMÁRIO DO INVENTO

O invento proporciona um método automático de processamento de correio electrónico, caracterizado por compreender a monitorização do tráfego de correio electrónico que passa através de um ou mais nós de uma rede a fim de detectar a disseminação de vírus previamente desconhecidos, compreendendo esta monitorização:

a) o registo de detalhes acerca das mensagens de correio electrónico numa base de dados; e

b) a pesquisa na base de dados de padrões de tráfego de correio electrónico que sejam indicativos de, ou sugerem, a disseminação de um vírus com origem em correio electrónico, através da aplicação de um conjunto predeterminado de critérios de suspeição a atributos (por exemplo, comprimento de mensagem, número de anexos, endereço de IP do emissor, resumo de primeiro anexo) das mensagens de correio electrónico, incluindo o conjunto de critérios que se referem a uma pluralidade de partes constituintes (por exemplo, linha de assunto, receptores, texto da mensagem, anexo) das mensagens de correio electrónico, e

uma vez detectado um padrão deste tipo, iniciar uma acção correctiva automática, alerta de um operador, ou ambas.

O invento também proporciona um sistema automático, numa ou para uma rede de computadores através do qual os utilizadores enviam mensagens de correio electrónico uns para os outros, para processamento de correio electrónico para detectar a disseminação de vírus previamente desconhecidos, compreendendo o sistema:

meios para monitorização do tráfego de correio electrónico que passa através de um ou mais nós da rede, cujos meios compreendem:

a) meios para registo de detalhes acerca das mensagens de correio electrónico numa base de dados; e

b) meios para pesquisa na base de dados de padrões de tráfego de correio electrónico que sejam indicativos de, ou sugiram, a disseminação de um vírus com origem em correio electrónico, pela aplicação de um conjunto predeterminado de critérios de suspeição a atributos (por exemplo comprimento de mensagem, número de anexos, endereço de IP do emissor, resumo de primeiro anexo) das mensagens de correio electrónico, incluindo o conjunto critérios que se referem a uma pluralidade de partes constituintes (por exemplo, linha de assunto, receptores, texto da mensagem) das mensagens de correio electrónico; e

meios operativos para, uma vez detectado um padrão deste tipo, iniciação da acção correctiva automática, alerta de um operador, ou ambas.

Deste modo, em vez da monitorização das mensagens de correio electrónico individuais, o invento trata as mensagens de correio electrónico processadas como um “conjunto” e procura padrões no tráfego de correio electrónico que sejam característicos de vírus que se propagam via correio electrónico. Foi determinado que padrões característicos deste tipo são relativamente fáceis de definir e de identificar uma vez que ocorram.

Para auxiliar na identificação de padrões relevantes de tráfego de correio electrónico, cada mensagem de correio electrónico é analisada por referência a um certo número de

critérios, que indicam que a mensagem de correio electrónico pode conter um vírus. Qualquer mensagem de correio electrónico que satisfaça qualquer destes critérios pode então ser registada numa base de dados. O exame de adições recentes a esta base de dados pode então ser utilizado para identificar padrões de tráfego indicativos ou que sugiram um ataque de vírus.

A decisão de registar ou não uma mensagem de correio electrónico particular pode ser tomada em função do mesmo satisfazer um ou mais critérios que indiquem que é possível que a mensagem de correio electrónico contenha um vírus. Por outras palavras, os critérios escolhidos para decidir registar uma mensagem de correio electrónico podem ser aqueles que indiquem que é possível que a mensagem de correio electrónico contenha um vírus, independentemente do mesmo o possuir na realidade, na base de que as mensagens de correio electrónico que não têm a possibilidade de conter um vírus não necessitam de ser registadas de forma individual. No entanto, o invento não exclui a possibilidade de que um ou mais critérios visem determinar se uma mensagem de correio electrónico na realidade contém um vírus, através de qualquer análise adequada, ou outra técnica analítica.

Admita-se que um utilizador relata que uma mensagem de correio electrónico particular contém um vírus como um anexo, e que o mesmo é um de um certo número de mensagens de correio electrónico que foi recentemente processado pelo sistema. A base de dados tem entradas que registam elementos tais como o emissor e o receptor, o assunto do correio electrónico, nomes e dimensões de anexos. Também é possível de modo automático (isto é, em suporte lógico) identificar os atributos relevantes armazenados destas mensagens e utilizar os mesmos como base para tomar acção correctiva em relação às mensagens de correio electrónico correspondentes, processadas subsequentemente. Também é possível notificar receptores de mensagens de correio electrónico correspondentes que tenham já sido processadas para tomarem acção correctiva por si próprios, por exemplo, para apagar o correio electrónico não lido e não aberto, assumindo que o sistema armazena o nome do receptor em texto simples.

DESCRIÇÃO DOS DESENHOS

O invento será também descrito por meio de exemplo não limitativo com referência aos desenhos anexos, em que:

a FIG. 1 ilustra o processo de envio de uma mensagem de correio electrónico através da Internet; e

a FIG. 2 é um diagrama de blocos de uma concretização do invento.

CONCRETIZAÇÃO ILUSTRADA

Antes de descrever a concretização ilustrada do invento, será descrito de forma resumida um processo típico de enviar uma mensagem de correio electrónico através da Internet com referência à FIG. 1. Isto é simplesmente para ilustração; existem vários métodos para entrega e recepção de correio electrónico através da Internet, incluindo, mas não limitado a: SMTP ponto a ponto, IMAP4 e UCCP. Existem também outras formas de conseguir SMTP para correio electrónico POP3, incluindo, por exemplo, a utilização de uma ligação por ISDN ou linha alugada em vez de uma ligação de marcação por modem.

Admita-se que um utilizador 1A com uma ID de correio electrónico “Asender” com a sua conta em “asource.com” deseja enviar uma mensagem de correio electrónico para alguém 1B com uma conta “arecipient” “adestination.com”, e que estes domínios .com são mantidos por ISP (fornecedores de serviço de Internet) respectivos. Cada um dos domínios tem um servidor de correio 2A, 2B que inclui um ou mais servidores SMTP 3A, 3B para mensagens que saem e um ou mais servidores POP3 4A, 4B para as que entram. Estes domínios fazem parte da Internet que para clareza é indicada separadamente em 5. O processo prossegue como se segue:

1. “Asender” prepara a mensagem de correio electrónico com a utilização de suporte lógico de cliente de correio electrónico 1A tal como o Microsoft Outlook Express e endereça a mesma para “arecipient@adestination.com”.

2. Utilizando uma ligação de marcação por modem ou semelhante, o cliente de correio electrónico do “Asender” 1A liga ao servidor de correio electrónico 2A em “mail.asource.com”.

3. O cliente de correio electrónico do “Asender” 1A conduz uma conversação com o servidor SMTP 3A, no decurso da qual o mesmo diz ao servidor SMTP 3A os endereços do emissor e do receptor e envia ao mesmo o corpo da mensagem (incluindo quaisquer anexos) transferindo deste modo a mensagem de correio electrónico 10 para o servidor 3A.

4. O servidor SMTP 3A analisa o campo TO do envelope de correio electrónico para a) o receptor e b) o nome de domínio do receptor. Assume-se que para as finalidades presentes que os ISP do emissor e do receptor são diferentes, caso contrário o servidor SMTP 3A poderia simplesmente redireccionar a mensagem de correio electrónico através do seu servidor(s) POP3 associado 4A para recolha subsequente.

5. O servidor SMTP 3A localiza um servidor de nome de domínio de Internet e obtém um endereço de IP para o servidor de correio do domínio de destino.

6. O servidor SMTP 3A liga ao servidor SMTP 3B em “adestination.com” via SMTP e envia ao mesmo os endereços do emissor e do receptor e o corpo da mensagem de forma semelhante ao Passo 3.

7. O servidor SMTP 3B reconhece que o nome de domínio se refere a si próprio e passa a mensagem para o servidor POP3 “adestination” 4B, o qual coloca a mensagem na caixa de correio “arecipient” para recolha pelo cliente de correio electrónico receptor 1B.

Existem várias formas nas quais pode ser utilizada a mensagem de correio electrónico para efeito maléfico, sendo provavelmente a mais amplamente conhecida um vírus que se desloca com a mensagem de correio electrónico como um anexo. Tipicamente, o receptor “ao abrir” o anexo, por duplo clique sobre o mesmo, possibilita que o vírus que pode ser um executável binário ou código de instruções escrito para um

intérprete alojado pelo cliente de correio electrónico ou pelo sistema operativo, executar. Nem o problema da intenção maléfica, nem a solução do presente invento para o mesmo, se restringem a vírus deste tipo. Por exemplo, outros ataques maléficos podem envolver a exploração de fraquezas do sistema de entrega (SMTP + POP3) ou do cliente de correio electrónico, como por formatação deliberada de um campo de cabeçalho de mensagem de correio electrónico numa forma que é conhecida por provocar mau funcionamento do suporte lógico que processa o mesmo.

Referindo agora a FIG. 2, esta mostra em forma de blocos os subsistemas chave de uma concretização do presente invento. No exemplo em consideração, isto é, o processamento da mensagem de correio electrónico por um ISP, estes subsistemas são implementados por suporte lógico executado no computador(s) do ISP. Estes computadores operam uma ou mais portas de interligação de correio electrónico 20A ... 20N que passam mensagens de correio electrónico tais como 10.

Os vários subsistemas da concretização serão descritos em maior detalhe abaixo mas de forma resumida compreendem:

- um decompositor/analisador de mensagem 21 que decompõe as mensagens de correio electrónico nas suas partes constituintes e analisa as mesmas para avaliar se as mesmas são candidatas a registo;

- um registador 22 que prepara uma entrada de base de dados para cada mensagem seleccionada como uma candidata a registo pelo decompositor/analisador 21;

- uma base de dados 23 que armazena as entradas preparadas pelo registador 22;

- um pesquisador 24 que analisa novas entradas na base de dados 23 para procurar sinais de tráfego que transporta vírus;

- um dispositivo de bloqueio 25 que sinaliza os resultados do pesquisador 24 e opcionalmente bloqueia a passagem de mensagens de correio electrónico conforme com

critérios do decompositor/analisador 21 que indiquem uma ameaça de vírus.

O dispositivo de bloqueio 25 pode ser implementado de uma forma tal que as mensagens de correio electrónico que são processadas pelo sistema e for considerado não infectado com um vírus pode ter uma notificação de texto inserida no mesmo, por exemplo, anexada ao texto da mensagem, dizendo que a mensagem de correio electrónico foi analisada pelo sistema, de modo que o receptor poderá ver o que a mesmo tem.

No global, o sistema da FIG. 2 funciona segundo os seguintes princípios.

Os vírus que se disseminam por correio electrónico podem ser detectados por exame dos padrões de tráfego do correio electrónico que os mesmos criam.

A concretização ilustrada aplica um conjunto de heurísticas para identificar vírus de correio electrónico. O que se segue é uma lista não exaustiva de critérios pelos quais as mensagens de correio electrónico podem ser avaliadas para implementar estas heurísticas. Outros critérios podem ser utilizados do mesmo modo ou em alternativa:

os mesmos contêm as mesmas linhas de assuntos ou semelhantes;

os mesmos contêm os mesmos textos de corpo ou semelhantes;

os mesmos contêm o mesmo anexo designado;

os mesmos contêm um anexo com o mesmo resumo de mensagem;

os mesmos são endereçados para muitos receptores;

os mesmos são endereçados para receptores por ordem alfabética ou alfabética inversa;

os mesmos são enviados para um endereço de correio electrónico particular e depois multiplicam as saídas do mesmo endereço de correio electrónico, e/ou endereços de correio electrónico semelhantes;

os mesmos contêm o mesmo formato estrutural;

os mesmos contêm as mesmas subtilezas estruturais;

os mesmos contêm os mesmos cabeçalhos de mensagem não habituais.

Os critérios acima deveriam ser auto explicativos, excepto possivelmente aqueles que se referem ao “resumo de mensagem” e a “subtilezas estruturais”; estas expressões são explicadas abaixo.

A cada um dos critérios acima é atribuído um resultado numérico. Cada mensagem de correio electrónico que passa através do sistema é analisada pelo decompositor/analisador 21 e registada numa base de dados 23 pelo registador 22. Uma rotina de pesquisa executada pelo pesquisador 24 de forma contínua analisa a nova informação que é armazenada na base de dados para ver se mensagens semelhantes estão a ser enviadas. Se as mesmas o forem, então a 'suspeita' da mensagem de correio electrónico é calculada com a utilização de um algoritmo que leva em consideração quão semelhantes são as mensagens e também como muitas das mesmas foram recebidas recentemente. Uma vez passado um limiar, todas as novas mensagens que correspondam aos critérios são bloqueadas como vírus potenciais pelo dispositivo de bloqueio 25 e um alarme é emitido.

O sistema pode gerar um resumo de mensagem, pelo menos para aquelas mensagens que estão registadas na base de dados. Os resumos de mensagem são um meio conveniente e eficiente de identificar mensagens com o mesmo texto de mensagem e como um “puxador” pelo qual se recupera uma recolha de entradas de registo que representam o mesmo texto de mensagem que é enviado em mensagens de correio electrónico múltiplas. O resumo pode ser armazenado na base de dados em adição, ou em alternativa, à lista de mensagens.

Um resumo de mensagem é tipicamente criado pela aplicação de algoritmos de Hash de sentido único (tais como MD5 ou Message-Digest-5) a uma série de caracteres (no caso presente, por exemplo, os caracteres de uma mensagem). As vantagens de utilizar um resumo nesta aplicação são:

- os mesmos são tipicamente menores do que a mensagem original e são de comprimento fixo, portanto os mesmos podem ser armazenados numa base de dados de forma mais fácil;

- os mesmos são tipicamente funções de sentido único, portanto a mensagem original não pode ser reconstruída, preservando deste modo a confidencialidade do utilizador;

- uma pequena alteração na mensagem resulta num resumo completamente diferente.

Por exemplo, o resumo MD5 de “The rain in spain falls mainly on the plain” é 6f7f4c35a219625efc5a9ebad8fa8527 e de “The rain in Spain falls mainly on the plain” é b417b67704f2dd2b5a812f99ade30e00. Estas duas mensagens diferem apenas por um bit (o 's' é Spain, uma vez que um S maiúsculo é um bit diferente de um s minúsculo no conjunto de caracteres ASCII), mas os resumos são totalmente diferentes.

Serão agora proporcionados alguns exemplos dos critérios pelos quais as mensagens de correio electrónico podem ser avaliadas:

Subtilezas estruturais: A maior parte das mensagens de correio electrónico é gerada por aplicações de experimentação e teste. Estas aplicações geram sempre a mensagem de correio electrónico com uma forma particular. É muitas vezes possível identificar que aplicação gerou uma mensagem de correio electrónico particular por averiguação dos cabeçalhos de correio electrónico e também por averiguação do formato das diferentes partes. É então possível identificar mensagens de correio electrónico que contenham subtilezas que indicam que o correio electrónico está a tentar parecer como se o mesmo fosse gerado por um emissor de correio electrónico conhecido, sem o ter sido, ou que o mesmo foi gerado por um novo e

desconhecido emissor de correio, ou por uma aplicação (que poderia ser um vírus ou verme). Todos são suspeitos.

Exemplos:

Escrita em maiúsculas inconsistente

de: alex@star.co.uk
Para: alex@star.co.uk

O de e o para têm diferentes escritas em maiúsculas

Ordem não padronizada dos elementos do cabeçalho

Assunto: tolerância a falhas da torre
Tipo de conteúdo: multipartes/misto; fronteira="======_962609498==_"
Mime-Version: 1.0

O cabeçalho Mime-Version normalmente vem antes do cabeçalho Content-Type.

Falta ou adição de elementos no cabeçalho

X-Mailer: QUALCOMM Windows Eudora Pro Version 3.0.5 (32)
Data: Seg, 03 Jul 2000 12:24:17 +0100
Eudora normalmente também inclui um cabeçalho X-Sender

Formato ID da mensagem

Mensagem-ID: <00270ibfe4elSb37dbdcOS9264010a@tomkins.int.star.co.uk>
X-Mailer: QUALCOMM Windows Eudora Pro Version 3.0.5 (32)

O cabeçalho X-mailer diz que o correio é gerado pelo Eudora, mas o formato id da mensagem é uma id de mensagem Outlook, não uma id de mensagem Eudora.

Formato da fronteira

X-Mailer: Microsoft Outlook 8.5, Build 4.71.2173.0
Tipo de conteúdo: multipartes/misto; fronteira = "======_962609498==_"

O cabeçalho X-mailer diz que o correio é gerado pelo Outlook, mas o formato da fronteira é uma fronteira Eudora, não uma fronteira Outlook.

Composição de quebra de linha e outro espaço em branco no cabeçalho da mensagem

Para: “Andrew Webley” <awebley@messagelabs.com>,
“Matt Cave” <MCave@messagelabs.com>,
“Alex at MessageLabs” ashipp@messagelabs.com
X-Mailer: QUALCOMM Windows Eudora Pro Version 3.0.5 (32)

O emissor de correio electrónico (Eudora) utiliza normalmente um espaço de um ponto e sem tabulação para linhas de continuação.

O mesmo tem origem em endereços de IP particulares ou em intervalos de endereços de IP.

O endereço de IP do emissor é, evidentemente, conhecido e deste modo pode ser utilizado para determinar se este critério é satisfeito.

O mesmo contém estruturas especializadas

Algum correio electrónico utiliza instruções HTML para cifrar o conteúdo da mensagem. Isto é destinado a anular analisadores linguísticos. Quando o correio é visto num cliente de correio tal como Outlook, o texto é imediatamente decifrado e exibido. Não seria habitual para uma mensagem de correio electrónico normal fazer isto.

Envelopes vazios de emissor de mensagens

Uma mensagem de correio electrónico normalmente indica o emissor no campo de texto de emissor e emissores de correio electrónico não desejado muitas vezes colocam uma entrada fictícia naquele campo para disfarçar o facto da mensagem de correio electrónico estar infectada. No entanto, a identidade do emissor também é suposta estar especificada no protocolo sob o qual SMTP processa a conversa para outro na transferência da mensagem de correio electrónico e este

critério é relativo à ausência da identificação do emissor do intervalo do protocolo relevante, designadamente o intervalo do protocolo *Mail From*.

Endereços inválidos de correio electrónico de emissor de mensagem

Isto é complementar ao elemento 8 e envolve a consideração tanto do campo emissor da mensagem como do intervalo do protocolo emissor, como se o mesmo fosse inválido. A mensagem de correio electrónico pode ser proveniente de um domínio que não existe ou não segue as regras normais para o domínio. Por exemplo, um endereço de HotMail de “123@hotmail.com” é inválido devido aos endereços de HotMail não poderem ser todos números.

Um certo número de campos da mensagem de correio electrónico pode ser examinado para entradas inválidas, incluindo “Sender”, “From”, e “Errors-to”.

Endereços de emissor de mensagem que não correspondem ao servidor de correio do qual é enviado o correio.

O servidor de correio local conhece, ou pelo menos pode determinar a partir do protocolo, o endereço do emissor do correio e deste modo pode ser determinado se este coincide com o endereço do emissor no texto do correio.

Numa implementação real do sistema da FIG. 2 uma rede de portas de interligação de correio electrónico 20 é preferida, para que a mensagem de correio electrónico possa ser processada na escala necessária. Quanto maior a disseminação desta rede e mais correio electrónico for processado, então maiores são as oportunidades de se poder interceptar vírus novos, reconhecer os sintomas e bloquear mais ocorrências antes do vírus se tornar demasiado disseminado. No entanto, a utilização de um certo número de portas de interligação de correio electrónico não é um componente essencial do sistema; o sistema pode reconhecer e detectar vírus novos mesmo se apenas uma porta de interligação de correio electrónico for utilizada e se mesmo uma pequena quantidade de correio electrónico passar através da mesma.

Todo o correio electrónico é feito passar através do analisador/decompositor 21, em que a mensagem de correio electrónico é separado nas suas partes constituintes. Para as finalidades de heurísticas de tráfego, cada parte é classificada como:

o cabeçalho de correio electrónico/cabeçalhos *mime*;

um componente normalmente considerado parte da mensagem;

um componente normalmente considerado como um anexo.

Cada parte é então mais analisada para ver se a mesma tem a possibilidade de conter ameaças potenciais.

Cabeçalho de correio electrónico/cabeçalhos *mime*: Linhas demasiado longas ou linhas com sintaxe não habitual podem ser utilizadas para rebentar motores de busca particulares, o que provoca quer uma recusa de assistência ao ataque quer uma exploração que pode provocar uma brecha na segurança ou disseminar um vírus.

Um componente normalmente considerado parte da mensagem: Estes podem conter código executável integrado. Por exemplo, uma mensagem HTML pode conter código de instruções em várias linguagens de computador ou a mesma pode conter elementos (tais como etiquetas <frameset> ou <object>) que foram mostrados para serem exploráveis.

Um componente normalmente considerado como um anexo: Estes podem ser directamente executáveis, tais como um ficheiro EXE. Os mesmos podem conter código executável integrado, tais como um documento Microsoft Word que contém uma macro. Os mesmos podem conter ficheiro de arquivo ou outros ficheiros recipiente, os quais podem conter outros componentes perigosos. Por exemplo, um ficheiro ZIP pode conter um executável.

Normalmente, o anexo tem de conter algum elemento executável para ser visto como uma ameaça potencial. No entanto, o sistema pode ser comutado para um modo onde o

mesmo vê todos os anexos como uma ameaça potencial. Isto é para fornecer duas possibilidades tais como:

Um documento, tal como uma imagem .jpg, pode conter formatação ilegal que rebente a aplicação utilizada para visualizar o anexo. Isto pode provocar quer uma recusa de assistência a ataque quer uma exploração que pode provocar uma brecha na segurança ou disseminar um vírus.

O corpo da mensagem pode conter instruções que, se seguidas, tornam o anexo numa forma perigosa, por exemplo, 'alterar o nome picture.jpg para picture.exe'.

Depois de analisar cada componente, então se qualquer um dos componentes tiver a possibilidade de conter uma ameaça potencial, a mensagem é registada pelo registador 22 na base de dados 23. Caso contrário a mensagem não é registada.

O registador 22 está programado para que o sistema registe componentes de cada mensagem para que mensagens semelhantes possam ser detectadas. Os seguintes são registados:

linha de assunto e resumo de linha de assunto;

poucos dos primeiros caracteres de parte de texto da mensagem de correio electrónico, resumo de primeira parte de texto e resumo de alguns primeiros caracteres;

nome de primeiro anexo;

resumo de primeiro anexo;

número de receptores;

se receptores estiverem por ordem alfabética ou ordem alfabética inversa;

tempo de registo;

resumo de emissor;

resumo de primeiro receptor;

indicadores de formato estrutural;

indicadores de subtileza estrutural;

cabeçalhos de mensagem não habituais;

tempo de chegada do correio electrónico.

A lista acima não é exaustiva e o invento não se restringe a esta combinação particular de elementos de informação.

A base de dados 23 regista detalhes sobre mensagens e possibilita consulta dos detalhes para encontrar padrões de mensagens de correio electrónico duplicadas ou semelhantes.

A fim de proporcionar capacidade de resposta, o registo pode ser uma operação a uma camada ou várias camadas. Por exemplo, mensagens podem ser registadas localmente numa base de dados geograficamente próxima dos servidores de correio electrónico e analisadas localmente. Isto dá uma resposta rápida a padrões de tráfego locais. No entanto, os registos podem também ser copiados para uma base de dados central para realizar análise global. Este será mais lento a reagir, mas pode reagir ao global, em vez de a padrões locais.

As entradas de registo anteriores são apagadas de modo automático da base de dados 23 uma vez que as mesmas deixam de ser necessárias - o sistema está concebido para proporcionar um aviso à priori de vírus novos.

O pesquisador 24 interroga periodicamente a base de dados à procura de mensagens semelhantes recentes e gera um resultado pela análise dos componentes. Em função do resultado, o sistema pode identificar uma ameaça 'definitiva' ou uma ameaça 'potencial'. Uma ameaça definitiva provoca uma assinatura para ser devolvida ao dispositivo de bloqueio para que todas as mensagens futuras com aquela característica

sejam bloqueadas. Uma ameaça potencial provoca um alerta para ser enviado a um operador que pode então decidir tratar como se a mesma fosse uma ameaça definitiva, assinalar como um alarme falso para que no futuro ocorrências sejam reportadas ou esperar e ver.

O pesquisador pode ser configurado com diferentes parâmetros, para que o mesmo possa ser mais sensível se pesquisar registos a partir de uma única porta de interligação de correio electrónico e menos sensível se processar uma base de dados de informação de todo o mundo.

A cada critério pode ser associado um resultado diferente.

O tempo entre pesquisas pode ser ajustado.

O intervalo de tempo que cada pesquisa cobre pode ser ajustado e múltiplos intervalos de tempos considerados.

Os limiares globais podem ser definidos.

O dispositivo de bloqueio 25 toma assinaturas do pesquisador 24. A assinatura identifica características de correio electrónico que tem de ser bloqueado. Ao receber a assinatura, todas as mensagens de correio electrónico futuras correspondentes são tratadas como vírus e bloqueadas.

Obviamente, a acção de bloqueio pode assumir um certo número de formas, que incluem:

- descarte das mensagens de correio electrónico infectadas sem enviar as mesmas para os seus receptores endereçados.

- retenção das mesmas em arquivo temporário e notificar os endereços por correio electrónico que uma mensagem infectada foi interceptada e está a ser retida durante um período para extracção, se os mesmos desejarem, caso contrário a mesma será apagada.

- desinfestação do correio electrónico por remoção da ameaça de vírus por quaisquer meios adequados; por exemplo, se o vírus for um anexo executável, o mesmo pode ser desanexado ou desactivado antes de fazer seguir a mensagem de correio electrónico para os seus endereços. A mensagem de correio electrónico pode ser modificada pela inclusão de uma mensagem de texto a dizer que a mensagem de correio electrónico foi desinfectada.

Quando um vírus é detectado, um servidor de correio automático 30 pode notificar outros sítios das características relevantes das mensagens de correio electrónico infectadas, quer para alertar operadores humanos quer para alimentar concretizações do invento em sítios remotos com as características das mensagens de correio electrónico necessárias para os seus dispositivos de bloqueio 25 para bloquearem as mesmas.

Algoritmo típico

O seguinte é um possível algoritmo que pode ser implementado pelo pesquisador 24 numa concretização ilustrada do invento.

Referindo o exemplo dos critérios de avaliação do correio electrónico expressos acima, será apreciado que uma mensagem de correio electrónico em consideração tem um certo número de atributos que podem ser representados como valores de dados num programa de computador, com o tipo de dados em função da natureza do atributo. Por exemplo, o comprimento da mensagem e o número de anexos são inteiros, enquanto que os vários cabeçalhos de texto (por exemplo, “To”, “SendTo”, “Subject”) são cadeias de caracteres, como são resumos tais como o resumo de mensagem. No que se segue, as mensagens de correio electrónico são consideradas como sendo iguais de acordo com um dado critério, se os atributos correspondentes forem iguais nos casos de inteiros e cadeias de caracteres. No caso de cadeias de caracteres, quando adequado, a igualdade pode ser determinada pela comparação da escrita em maiúsculas; comparações da escrita em maiúsculas são adequadas para campos de texto de uma mensagem de correio

electrónico, mas não necessariamente para outras cadeias de caracteres. (No caso de um atributo representado por um valor em vírgula flutuante, uma pessoa especializada poderá perceber que comparações deverão ser feitas em função do valor absoluto da diferença ser maior do que algum valor pequeno arbitrário, algumas vezes referido como “épsilon” na literatura técnica, o qual é, ele próprio, maior do que o erro de arredondamento).

Abaixo, os números entre parêntesis são números de passo para identificar os passos concretizados.

Em intervalos regulares (100):

Para cada critério A mede-se (110)

Para cada intervalo de tempo de B minutos mede-se (200)

Tomar o conjunto de amostras S das mensagens de correio electrónico ao longo dos últimos minutos B, quando o seu valor de acordo com um critério seleccionado A for igual (210). Efectuar a partição do conjunto de amostra se o mesmo contém valores que não podem ser o mesmo vírus (por exemplo, se algumas mensagens de correio electrónico no conjunto contêm instruções HTML e algumas contêm um EXE, este não pode ser o mesmo vírus e cada uma deverá ser tratada como um conjunto separado S pelo passo 210)

Para cada conjunto de amostra S (300)

Definir X = número de correios no conjunto de amostra (310)

Multiplicar X do passo 310 por um factor de importância C para o critério A (320). Cada critério tem um factor de importância respectivo que depende da natureza do critério, uma vez que alguns critérios, por exemplo, o nome de um anexo de ficheiro podem ser mais

significativos do que outros tanto quanto a avaliação da probabilidade de uma ameaça de vírus é preocupante; comentários semelhantes aplicam-se aos outros factores referidos abaixo)

Adicionar a X do passo 320 um segundo factor de importância D para cada outro critério A2, onde A2 também é igual ao longo do conjunto de amostra S (330)

Adicionar a X do passo 330 um terceiro factor de importância E para cada outro critério A3, onde A3 tem um conjunto limitado de diferentes valores ao longo do conjunto de amostra S (340). Meios de “Intervalo limitado” > 1 e < R. Cada intervalo de tempo B tem um R respectivo.

Adicionar a X do passo 340 um factor de disseminação (P vezes T) se o conjunto de amostras contém Q mensagens de correio electrónico que entram num domínio e então T cópias que deixam o domínio (onde T > Q) (350). Cada intervalo de tempo B tem um P e Q diferentes.

Se X do passo 350 for maior do que o limiar V (cada intervalo de tempo B tem um limiar V respectivo) então assinalar como vírus (360).

Caso contrário

Se X do passo 350 for maior do que o limiar O (cada intervalo de tempo B tem um limiar O respectivo), onde O é inferior a V, então assinalar como necessária a assistência do operador (370). O operador pode então avaliar se uma ameaça de vírus está presente ou não e instruir o suporte lógico para proceder em conformidade.

Conjunto de amostra seguinte (380)

Intervalo seguinte (210)

Critério seguinte (120)

Note que os três factores de "importância" C, D, E, o factor de disseminação e os limiares são valores numéricos que podem ser definidos empiricamente e podem ser ajustados de forma dinâmica. Também, o algoritmo pode ser concretizado utilizando um ou mais valores diferentes para o intervalo de tempo B, por exemplo, 5 minutos, 30 minutos e 180 minutos.

Em Inglês: procuram-se mensagens de correio electrónico com características semelhantes que chegam num dado período de tempo. Quanto mais semelhantes forem as mensagens de correio electrónico encontradas, mais suspeitas se tornam. Se as mensagens de correio electrónico também tiverem outra característica em comum, isto torna as mesmas ainda mais suspeitas.

Algumas coisas podem ser mais suspeitas do que outras - por exemplo, pode-se escolher reservar um resultado mais elevado se forem vistas mensagens de correio electrónico com o mesmo nome de anexo, do que se forem vistas mensagens de correio electrónico com a mesma linha de assunto.

Se forem vistas mensagens de correio electrónico que são enviadas para um domínio e depois chegar uma inundação, isto é também suspeito.

Ainda que, acima, o invento tenha sido descrito com referência à sua aplicação a correio electrónico de internet, o mesmo não se restringe a este tipo de correio electrónico; o invento é igualmente aplicável a outras redes privadas ou públicas, locais ou de área alargada ou a combinações destes tipos de redes com outras e com a Internet, bem como a correio electrónico através de WAP (protocolo de acesso sem fios) e SMS (serviço de mensagens simples) para telefones móveis e dispositivos semelhantes.

Lisboa,

REIVINDICAÇÕES

1 - Método automático de processamento de correio electrónico, caracterizado por compreender a monitorização do tráfego de correio electrónico que passa através de um ou mais nós de uma rede a fim de detectar a disseminação de vírus previamente desconhecidos, compreendendo esta monitorização:

a) o registo (22) de detalhes acerca das mensagens de correio electrónico numa base de dados (23); e

b) a pesquisa (24) na base de dados de padrões de tráfego de correio electrónico que são indicativos de, ou sugerem, a disseminação de um vírus com origem em correio electrónico, pela aplicação a um conjunto predeterminado de critérios de suspeição a atributos, por exemplo, comprimento de mensagem, número de anexos, endereço de IP do emissor, resumo do primeiro anexo das mensagens de correio electrónico, incluindo o conjunto critérios que se referem a uma pluralidade de partes constituintes, por exemplo, linha de assunto, receptores, texto da mensagem, anexo das mensagens de correio electrónico, e

uma vez detectado um padrão, iniciação (25) de acção correctiva automática, alerta de um operador, ou ambas.

2 - Método de acordo com a reivindicação 1, em que no passo b) diferentes factores numéricos de importância são aplicados a diferentes critérios de suspeição.

3 - Método de acordo com a reivindicação 1 ou 2, em que, durante a aplicação do conjunto predeterminado de critérios de suspeição, é atribuído a um conjunto de mensagens de correio electrónico um resultado numérico, calculado de acordo com uma combinação seleccionada dos ditos critérios e é assinalado como tendo vírus se o resultado exceder um limiar predeterminado.

4 - Método de acordo com a reivindicação 3, em que, se o resultado não exceder o dito limiar mas exceder um segundo

limiar, inferior, o conjunto de mensagens de correio electrónico é assinalado para a atenção de um operador.

5 - Método de acordo com qualquer uma das reivindicações 1 a 4, em que o registo da mensagem de correio electrónico inclui o registo de um resumo:

do texto da mensagem;

da linha de assunto;

de poucos dos primeiros caracteres da parte de texto da mensagem de correio electrónico;

da primeira parte de texto da mensagem de correio electrónico;

do primeiro anexo;

do emissor; ou

do primeiro receptor.

6 - Método de acordo com qualquer uma das reivindicações 1 a 5, em que um dos ditos critérios é que uma mensagem de correio electrónico contenha escrita em maiúsculas inconsistente.

7 - Método de acordo com qualquer uma das reivindicações 1 a 6, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha uma composição de quebra de linha ou outro espaço em branco nos cabeçalhos de mensagem inconsistente com o emissor indicado da mensagem de correio electrónico.

8 - Método de acordo com qualquer uma das reivindicações 1 a 7, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha ordem não padronizada dos elementos do cabeçalho.

9 - Método de acordo com qualquer uma das reivindicações 1 a 8, em que um dos ditos critérios é que uma

mensagem de correio electrónico tenha elementos de cabeçalho em falta ou adicionais.

10 - Método de acordo com qualquer uma das reivindicações 1 a 9, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha informação de ID de mensagem inconsistente.

11 - Método de acordo com qualquer uma das reivindicações 1 a 10, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha um formato de fronteira inconsistente com o gerador indicado do mensagem de correio electrónico.

12 - Método de acordo com qualquer uma das reivindicações 1 a 11, em que um dos ditos critérios é que a parte da mensagem de uma mensagem de correio electrónico esteja cifrada para impedir análise linguística.

13 - Método de acordo com qualquer uma das reivindicações 1 a 12, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha um envelope de emissor de mensagem vazio.

14 - Método de acordo com qualquer uma das reivindicações 1 a 13, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha um endereço de emissor de mensagem inválido.

15 - Método de acordo com qualquer uma das reivindicações 1 a 14, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha um endereço de emissor de mensagem que não corresponde com o servidor de correio a partir do qual a mesma foi enviada.

16 - Método de acordo com qualquer uma das reivindicações 1 a 15, em que um dos ditos critérios é que as mensagens de correio electrónico estejam endereçadas para receptores por ordem alfabética ou ordem alfabética inversa.

17 - Método de acordo com qualquer uma das reivindicações 1 a 16, em que um dos ditos critérios é que as

mensagens de correio electrónico sejam enviadas para um endereço de correio electrónico particular e depois multipliquem as saídas do mesmo endereço de correio electrónico e/ou de endereços de correio electrónico semelhantes.

18 - Método de acordo com qualquer uma das reivindicações 6 a 17, em que um dos ditos critérios é que as mensagens de correio electrónico contenham o mesmo formato estrutural.

19 - Método de acordo com qualquer uma das reivindicações 1 a 18, em que um dos ditos critérios é que as mensagens de correio electrónico contenham os mesmos cabeçalhos não habituais.

20 - Método de acordo com qualquer uma das reivindicações 1 a 19, em que um dos ditos critérios é que as mensagens de correio electrónico contenham a mesma subtileza estrutural.

21 - Método de acordo com qualquer uma das reivindicações anteriores, em que um dos ditos critérios é que uma mensagem de correio electrónico seja originada num endereço de IP particular ou num endereço numa gama de endereços de IP.

22 - Método de acordo com qualquer uma das reivindicações anteriores, em que os detalhes de uma mensagem de correio electrónico não são registados se a análise da mensagem de correio electrónico determinar que não é possível que a mensagem de correio electrónico contenha um vírus.

23 - Método de acordo com qualquer uma das reivindicações anteriores, em que a pesquisa examina, principal ou exclusivamente, apenas as entradas da base de dados adicionadas recentemente, isto é, as entradas que tenham sido adicionadas há menos do que um período de tempo predeterminado.

24 - Método de acordo com qualquer uma das reivindicações anteriores, em que a acção correctiva inclui

qualquer ou todos dos seguintes, em relação a cada mensagem de correio electrónico de acordo com o padrão detectado:

a) bloqueio, pelo menos, temporário da passagem da mensagem de correio electrónico

b) notificação do emissor da mensagem de correio electrónico

c) notificação do receptor(s) de destino da mensagem de correio electrónico

d) desinfestação da mensagem de correio electrónico

e) geração de um sinal para alertar um operador humano.

25 - Método de acordo com qualquer uma das reivindicações anteriores e que inclui o envio de uma mensagem de identificação de mensagens de correio electrónico suspeitas para um servidor de correio electrónico automático.

26 - Método de acordo com qualquer uma das reivindicações anteriores e que inclui o passo de processamento de mensagens de correio electrónico infectadas para desinfectar as mesmas ou desactivar um vírus nas mesmas.

27 - Método de acordo com qualquer uma das reivindicações anteriores e que inclui o passo de inserção nas mensagens de correio electrónico tidas como não infectadas por vírus, de uma mensagem que indica que a mensagem de correio electrónico foi processada.

28 - Sistema automático, numa ou para uma rede de computadores, através da qual os utilizadores enviam mensagens de correio electrónico uns para os outros, para processamento de correio electrónico para detectar a disseminação de vírus previamente desconhecidos, compreendendo o sistema:

meios para monitorização do tráfego de correio electrónico que passa através de um ou mais nós da rede, cujos meios compreendem:

a) meios para registo (22) de detalhes acerca das mensagens de correio electrónico numa base de dados (23), e

b) meio para pesquisa (24) na base de dados de padrões de tráfego de correio electrónico que sejam indicativos de, ou sugiram, a disseminação de um vírus com origem em correio electrónico, pela aplicação de um conjunto predeterminado de critérios de suspeição a atributos, por exemplo, comprimento de mensagem, número de anexos, endereço de IP do emissor, resumo de primeiro anexo das mensagens de correio electrónico, incluindo o conjunto critérios que se referem a uma pluralidade de partes constituintes, por exemplo, linha de assunto, receptores, texto de mensagem das mensagens de correio electrónico; e

meios operativos para, uma vez detectado um padrão, iniciação (25) de acção correctiva automática, alerta de um operador, ou ambas.

29 - Sistema de acordo com a reivindicação 28, em que na operação dos meios b) diferentes factores numéricos de importância são aplicados a diferentes critérios de suspeição.

30 - Sistema de acordo com a reivindicação 28 ou 29, em que, durante a aplicação do conjunto predeterminado de critérios de suspeição, é atribuído a um conjunto de mensagens de correio electrónico um resultado numérico, calculado de acordo com uma combinação seleccionada dos ditos critérios e é assinalado como tendo vírus se o resultado exceder um limiar predeterminado.

31 - Sistema de acordo com a reivindicação 30, em que, se o resultado não exceder o dito limiar mas exceder um segundo limiar, inferior, o conjunto de mensagens de correio electrónico é assinalado para a atenção de um operador.

32 - Sistema de acordo com qualquer uma das reivindicações 28 a 31, em que o registo da mensagem de correio electrónico inclui o registo de um resumo:

do texto da mensagem;

da linha de assunto;

de poucos dos primeiros caracteres da parte de texto da mensagem de correio electrónico;

da primeira parte de texto da mensagem de correio electrónico;

do primeiro anexo;

do emissor; ou

do primeiro receptor.

33 - Sistema de acordo com qualquer uma das reivindicações 28 a 32, em que um dos ditos critérios é que uma mensagem de correio electrónico contenha escrita em maiúsculas inconsistente.

34 - Sistema de acordo com qualquer uma das reivindicações 28 a 33, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha uma composição de quebra de linha ou outro espaço em branco nos cabeçalhos de mensagem inconsistente com o emissor indicado da mensagem de correio electrónico.

35 - Sistema de acordo com qualquer uma das reivindicações 28 a 34, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha ordem não padronizada dos elementos do cabeçalho.

36 - Sistema de acordo com qualquer uma das reivindicações 28 a 35, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha elementos no cabeçalho em falta ou adicionais.

37 - Sistema de acordo com qualquer uma das reivindicações 28 a 36, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha informação de ID de mensagem inconsistente.

38 - Sistema de acordo com qualquer uma das reivindicações 28 a 37, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha um formato de fronteira inconsistente com o gerador indicado do correio electrónico.

39 - Sistema de acordo com qualquer uma das reivindicações 28 a 38, em que um dos ditos critérios é que a parte da mensagem de uma mensagem de correio electrónico esteja cifrada para impedir a análise linguística.

40 - Sistema de acordo com qualquer uma das reivindicações 28 a 39, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha um envelope de emissor de mensagem vazio.

41 - Sistema de acordo com qualquer uma das reivindicações 28 a 40, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha um endereço de emissor de mensagem inválido.

42 - Sistema de acordo com qualquer uma das reivindicações 28 a 41, em que um dos ditos critérios é que uma mensagem de correio electrónico tenha um endereço de emissor de mensagem que não corresponde com o servidor de correio a partir do qual a mesma foi enviada.

43 - Sistema de acordo com qualquer uma das reivindicações 28 a 42, em que um dos ditos critérios é que as mensagens de correio electrónico estejam endereçadas para receptores por ordem alfabética ou ordem alfabética inversa.

44 - Sistema de acordo com qualquer uma das reivindicações 28 a 43, em que um dos ditos critérios é que as mensagens de correio electrónico sejam enviadas para um endereço particular de correio electrónico e depois multipliquem as saídas do mesmo endereço de correio electrónico e/ou de endereços de correio electrónico semelhantes.

45 - Sistema de acordo com qualquer uma das reivindicações 33 a 44, em que um dos ditos critérios é que

as mensagens de correio electrónico contenham o mesmo formato estrutural.

46 - Sistema de acordo com qualquer uma das reivindicações 28 a 45, em que um dos ditos critérios é que as mensagens de correio electrónico contenham os mesmos cabeçalhos não habituais.

47 - Sistema de acordo com qualquer uma das reivindicações 28 a 46, em que um dos ditos critérios é que as mensagens de correio electrónico contenham a mesma subtileza estrutural.

48 - Sistema de acordo com qualquer uma das reivindicações 28 a 47, em que um dos ditos critérios é que uma mensagem de correio electrónico seja originado num endereço de IP particular ou num endereço numa gama de endereços de IP.

49 - Sistema de acordo com qualquer uma das reivindicações 28 a 48, em que, durante a operação dos ditos meios, os detalhes de uma mensagem de correio electrónico não são registados se a análise da mensagem de correio electrónico determinar que não é possível que a mensagem de correio electrónico contenha um vírus.

50 - Sistema de acordo com qualquer uma das reivindicações 28 a 49, em que, em operação, a pesquisa examina, principal ou exclusivamente, apenas as entradas da base de dados adicionadas recentemente, isto é, entradas que tenham sido adicionadas há menos do que um período de tempo predeterminado.

51 - Sistema de acordo com qualquer uma das reivindicações 28 a 50, em que os meios de iniciação funcionam de modo que a acção correctiva inclui qualquer ou todos dos seguintes, em relação a cada mensagem de correio electrónico de acordo com o padrão detectado:

a) bloqueio, pelo menos, temporário da passagem da mensagem de correio electrónico

b) notificação do emissor da mensagem de correio electrónico

c) notificação do receptor(s) de destino da mensagem de correio electrónico

d) desinfestação da mensagem de correio electrónico

e) geração de um sinal para alertar um operador humano.

52 - Sistema de acordo com qualquer uma das reivindicações 28 a 51 e que inclui meios para envio de uma mensagem de identificação de mensagens de correio electrónico suspeitas para um servidor de correio electrónico automático.

53 - Sistema de acordo com qualquer uma das reivindicações 28 a 52 e que inclui meios para processamento de mensagens de correio electrónico infectadas para desinfectar as mesmas ou desactivar um vírus nas mesmas.

54 - Sistema de acordo com qualquer uma das reivindicações 28 a 53 e que inclui meios para inserção nas mensagem de correio electrónico tido como não infectado por vírus, de uma mensagem que indica que a mensagem de correio electrónico foi processada.

Lisboa,

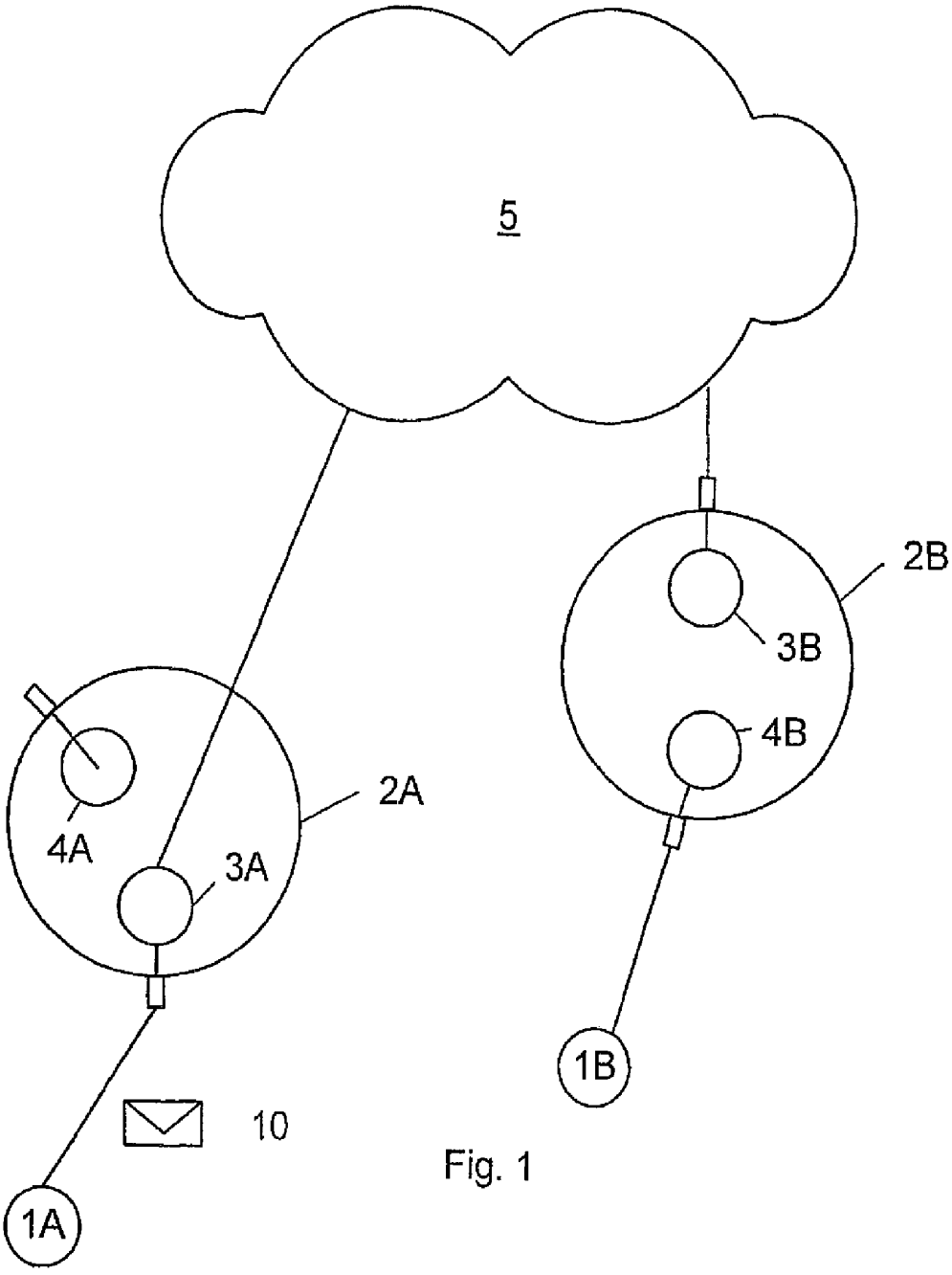


Fig. 1

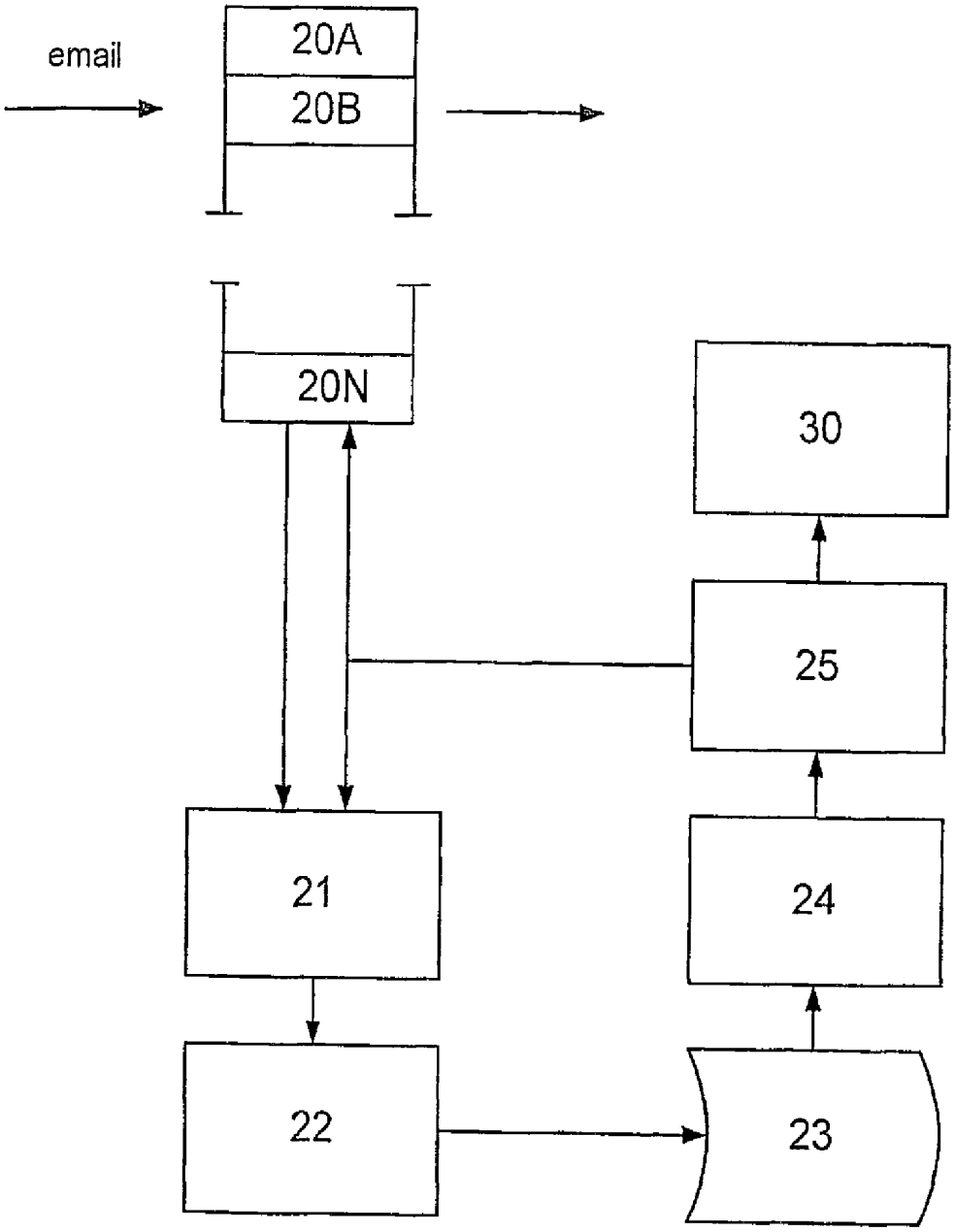


Fig. 2