

LIV - Linux Integrated Viruswall

Teobaldo Adelino Dantas de Medeiros
GEINF - CEFET/RN
Av. Senador Salgado Filho 1559, Tirol
59015-000 Natal – RN
teobaldo@cefetrn.br

Paulo Sérgio da Motta Pires
DCA – UFRN
Centro de Tecnologia
59072-970 Natal –RN
pmotta@dca.ufrn.br

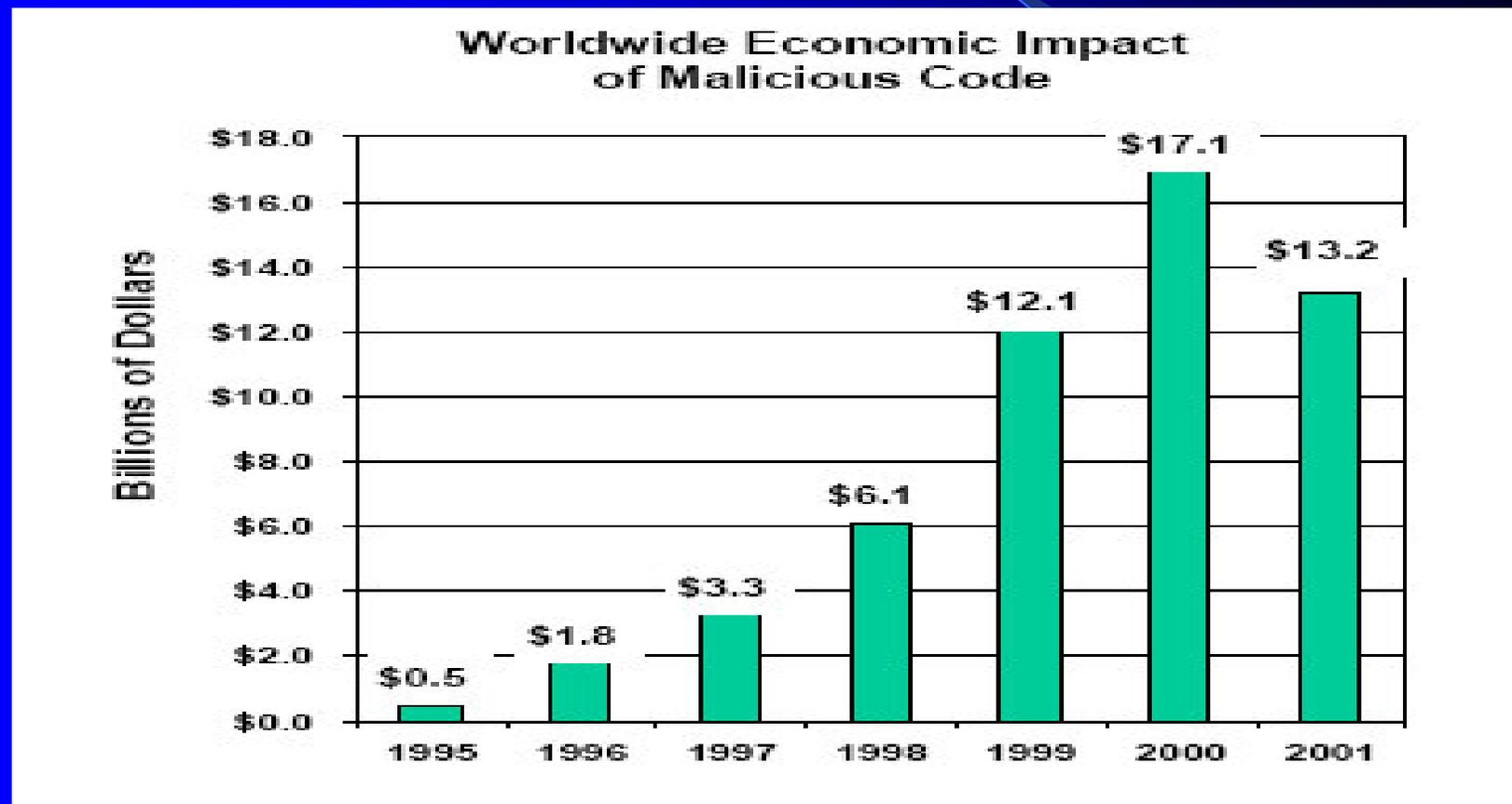
AGENDA

- 1) Agentes Maliciosos e Antivírus
- 2) O LIV
- 3) Mecanismos de Detecção e Contenção de Agentes Maliciosos do LIV
- 4) Resultados Obtidos
- 5) Conclusões

- 1 -

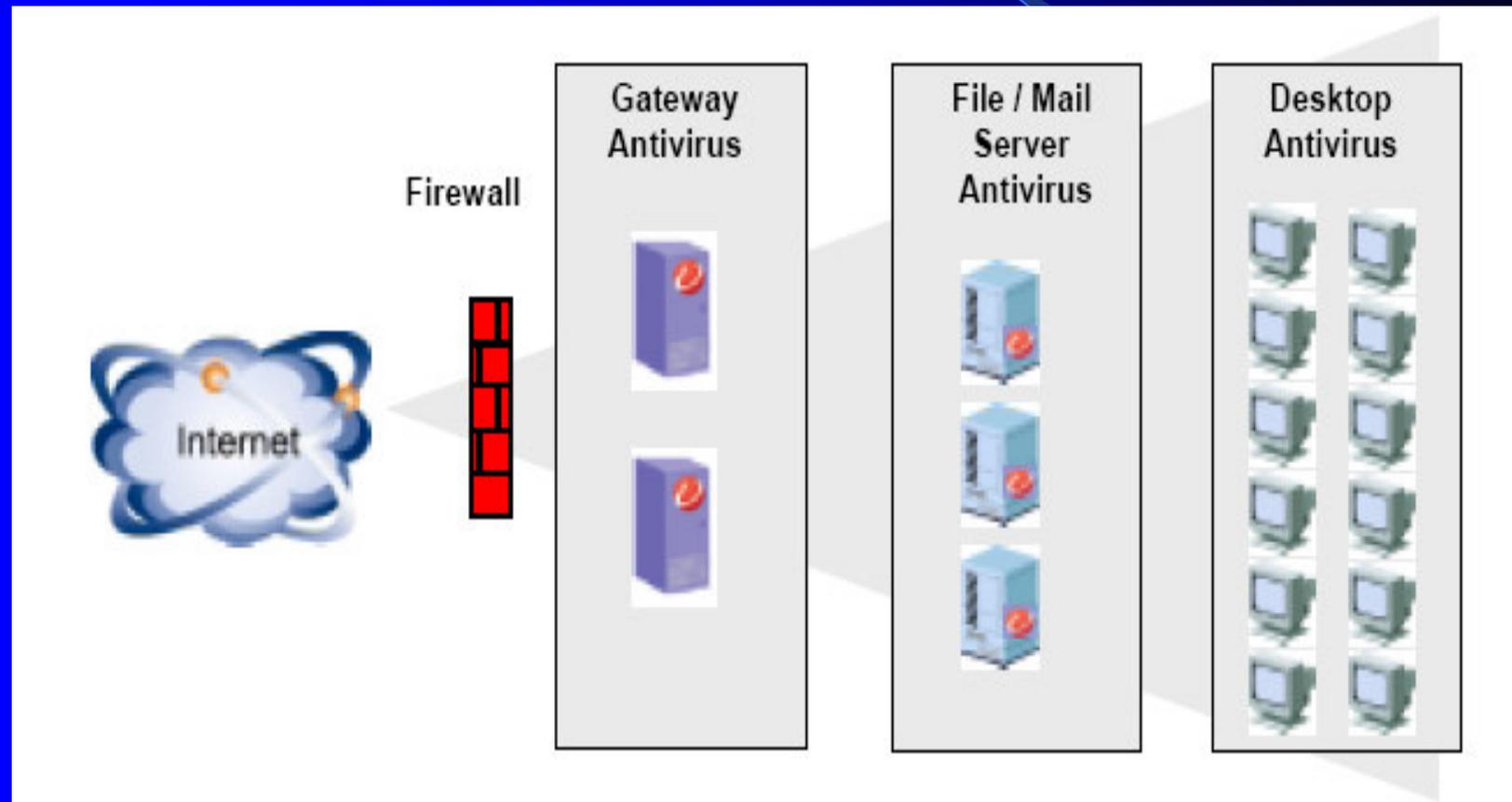
Agentes Maliciosos e Antivírus

1.1 Impacto Econômico da Ação dos Agentes Maliciosos



Fonte: Computer Economics, 2002 e 2003

1.2 Modelo de Proteção Contra Agentes Maliciosos



Fonte: Trend Micro

1.3 Problemas

CERT[®] Incident Note IN-2003-01

Several recent malicious code incidents (...) have achieved widespread propagation at rates significantly faster than many previous viruses. This increase speed is, unfortunately, also faster than many antivirus signatures can be identified and updated, regardless of the update method.

1.4 Outros Problemas

- Administração da estação de trabalho e do antivírus pelo usuário final;
- Existência de estações de trabalho vulneráveis na rede;
- Caso alguma estação vulnerável seja contaminada, o agente malicioso propagar-se-á para outras estações via compartilhamentos de rede ou e-mail interno da organização.

-2 -

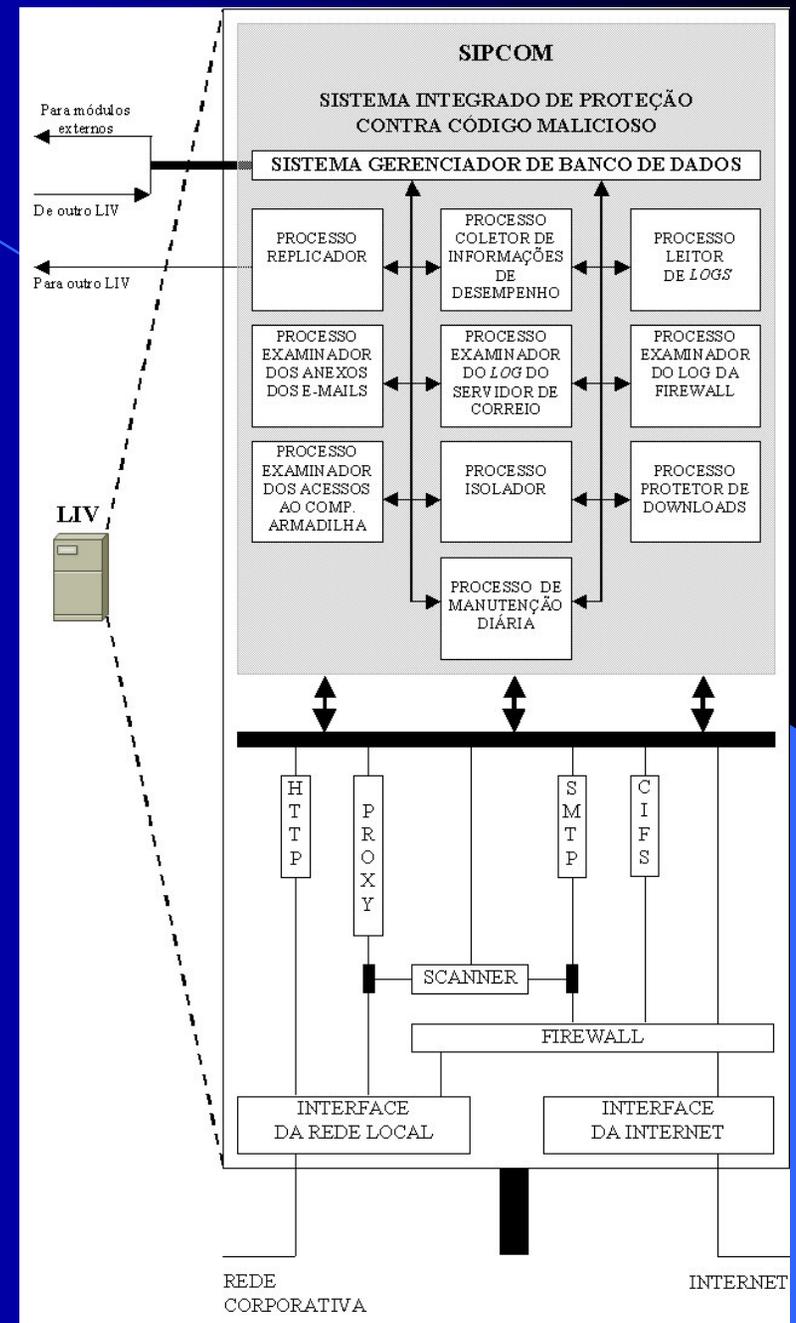
Linux integrated Viruswall

2.1 Características

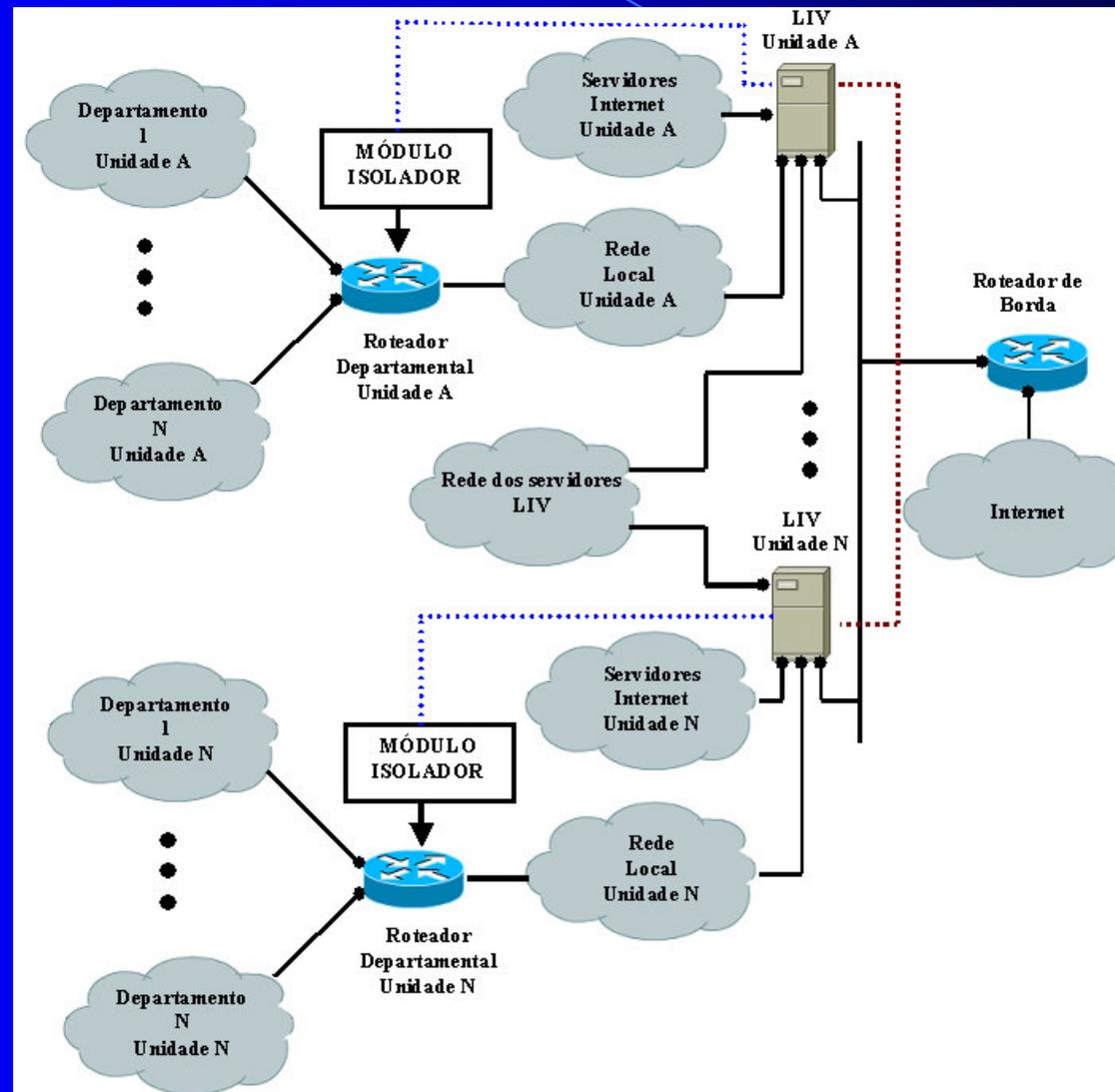
1. Filtro SMTP, FTP e HTTP;
2. Detecção de estações contaminadas através da análise do tráfego da rede;
3. Uso da técnica de “compartilhamento-armadilha” para rastrear a propagação de agentes maliciosos pela rede local;
4. Isolamento das estações de trabalho contaminadas;
5. Configuração via WEB.

2.2 Arquitetura LIV

- SIPCOM – Composto de 11 processos que coordenam o funcionamento do LIV;
- Servidores: HTTP – *Apache*, PROXY – *Squid*, SMTP – *SendMail*, CIFS – *Samba*;
- Servidor de Banco de Dados – *MySQL*;
- Firewall do Kernel Linux;
- *Scanner* Antivírus



2.3 Topologia da Rede com o LIV



- 3 -

Mecanismos de Detecção e Contenção de Agentes Maliciosos do LIV

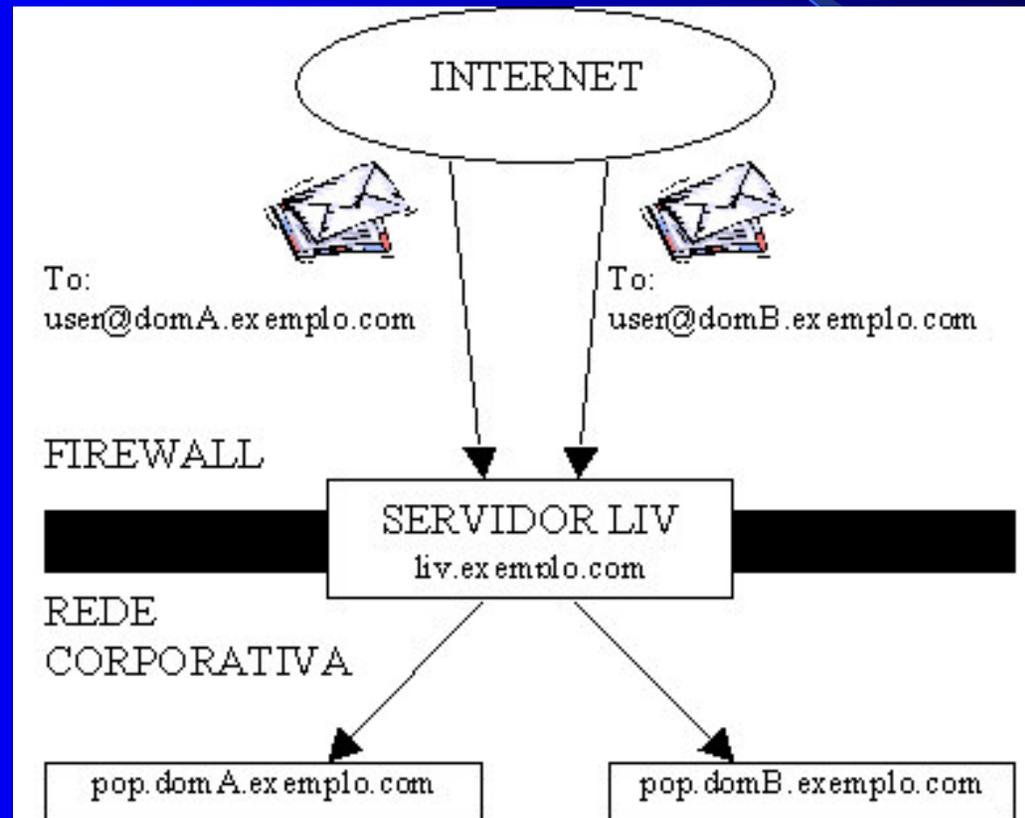
3.1 Mecanismos Usados pelo LIV para Detectar e Conter Agentes Maliciosos

- Filtragem de Tráfego SMTP, HTTP e FTP;
- Exame do Tráfego de Rede Local e dos Acessos aos Servidores de Correio;
- Uso do Compartilhamento-Armadilha;
- Isolamento de Estações de Trabalho Contaminadas.

3.1.1 A Filtragem do Tráfego SMTP

- Remove Anexos Infectados;
- Isola estações da rede local transmitindo agentes maliciosos;
- Cria lista dinâmica de endereços de correio transmissores de agentes maliciosos;
- Impede a entrada de extensões de arquivo potencialmente perigosas em anexos.

3.1.2 Funcionamento do Filtro SMTP



3.1.3 Filtragem de Extensões de Arquivos em Anexos



The screenshot displays the web interface of the Linux Integrated Viruswall (LIV). The browser window title is "LIV - Linux Integrated Viruswall - Microsoft Internet Explorer". The main navigation bar includes "CONSULTAS", "INFORMAÇÕES", "ESTATÍSTICAS", "ADMINISTRAÇÃO", and "LOGOUT (TEOBALDO)". The left sidebar contains several menu items: "CONFIGURAÇÃO GERAL", "DEFINIÇÃO DE PADRÕES", "PARCEIROS LIV", "EXCLUSÃO DE ISOLAMENTO", "EXTENSÕES PERIGOSAS", "ROTEADORES DA REDE", and "BANCO DE DADOS". The main content area is titled "Extensões Perigosas LIV" and contains a table with the following data:

| # | Extensão | Ação |
|----|----------|--------------------|
| 1 | 386 | [Liberar][Remover] |
| 2 | BAT | [Liberar] |
| 3 | BIN | [Liberar][Remover] |
| 4 | CLASS | [Liberar][Remover] |
| 5 | CMD | [Liberar][Remover] |
| 6 | COM | [Liberar] |
| 7 | DLL | [Liberar] |
| 8 | DRV | [Liberar][Remover] |
| 9 | EML | [Liberar] |
| 10 | EXE | [Liberar] |
| 11 | INF | [Liberar][Remover] |

3.1.4 Filtragem de Tráfego HTTP e FTP

- Mecanismo implementado no servidor *proxy* (SQUID);
- Após o *download* de arquivos contendo extensões predefinidas (.exe, .com, .zip, etc.), um *scanner* é ativado.
- Somente arquivos livres de agentes maliciosos conhecidos são repassados aos usuários.

3.2 Exame do Tráfego de Rede Local e dos Acessos aos Servidores de Correio

- Detecta padrões suspeitos no tráfego de rede local das estações de trabalho ou nos acessos realizados aos servidores de correio.
- Os padrões são definidos através de regras inseridas pelo administrador do LIV.
- As regras, por sua vez, são compostas de um conjunto de atributos.

3.2.1 As Regras do Servidor LIV

- O LIV utiliza regras criadas pelo administrador para detectar estações que estejam gerando padrões de tráfego suspeitos na rede;
- Os pacotes de rede ou os acessos ao servidor de correio que estejam relacionados às regras são registrados pelo LIV em banco de dados;
- Periodicamente o LIV consulta o banco de dados e isola as estações que estejam gerando os padrões indicados pelas regras.

3.2.2 Atributos das Regras - Rede

- Porta de Destino;
- Protocolo;
- Número Máximo de Conexões ao Servidor LIV;
- Número Máximo de Conexões a Endereços da Intranet;
- Número Máximo de Conexões a Endereços da Internet;
- Número Máximo de Destinos Distintos;
- Número Máximo de Acessos Periódicos;
- Intervalo.

3.2.3 Exemplo - Regras para o Tráfego de Rede

The screenshot shows a web browser window titled "LIV - Linux Integrated Viruswall - Microsoft Internet Explorer". The browser's menu bar includes "Arquivo", "Editar", "Exibir", "Favoritos", "Ferramentas", and "Ajuda". The main content area displays the "LIV - Linux Integrated Viruswall" interface with a navigation menu on the left and a main panel titled "Consulta Regras Firewall".

The navigation menu on the left contains the following items:

- CONFIGURAÇÃO GERAL
- DEFINIÇÃO DE PADRÕES
- PARCEIROS LIV
- EXCLUSÃO DE ISOLAMENTO
- EXTENSÕES PERIGOSAS
- ROTEADORES DA REDE
- BANCO DE DADOS

The main panel "Consulta Regras Firewall" features a table with the following columns: Pacote, Destino, Máximos, Tempo, and Ação. The table contains 6 rows of data and a final row for adding a new rule.

| # | Pacote | | Destino | | | Máximos | | Tempo | Ação |
|---|--------|-------|---------|------|------|---------|------|----------|--------------|
| | Porta | Prot. | LIV | Rede | Int. | Dist. | Per. | Interv. | |
| 1 | 135 | TCP | 10 | 100 | 50 | 20 | 5 | 02:00:00 | [Des.][Alt.] |
| 2 | 445 | TCP | 10 | 100 | 50 | 20 | 5 | 02:00:00 | [Des.][Alt.] |
| 3 | 139 | TCP | 10 | | 50 | 40 | 5 | 02:00:00 | [Des.][Alt.] |
| 4 | 25 | TCP | 50 | 5 | 50 | 5 | 8 | 02:00:00 | [Des.][Alt.] |
| 5 | 137 | UDP | 10 | 1000 | 100 | 20 | 5 | 02:00:00 | [Des.][Alt.] |
| 6 | 138 | UDP | 10 | 1000 | 100 | 20 | 5 | 02:00:00 | [Des.][Alt.] |
| # | | TCP | | | | | | | [Incluir] |

At the bottom of the main panel, there are two links: [Topo] and [Voltar].

3.2.4 Atributos das Regras - Servidor de Correio

- Número Máximo de Endereços Eletrônicos de Origem para o Mesmo IP Originador;
- Número Máximo de Endereços Eletrônicos de Destino para o Mesmo IP Originador;
- Número Máximo de Mensagens para o Mesmo Endereço Eletrônico por IP Originador;
- Número Máximo de Mensagens com Endereço de Origem Externo por IP Originador;
- Intervalo.

3.2.5 Exemplo - Regras para o Servidor de Correio



The screenshot shows a web browser window titled "LIV - Linux Integrated Viruswall - Microsoft Internet Explorer". The browser's menu bar includes "Arquivo", "Editar", "Exibir", "Favoritos", "Ferramentas", and "Ajuda". The main content area displays the "LIV - Linux Integrated Viruswall" logo and a navigation menu with options: "CONSULTAS", "INFORMAÇÕES", "ESTATÍSTICAS", "ADMINISTRAÇÃO", and "LOGOUT (TEOBALDO)".

The main content area is titled "Consulta Regras Email" and features a table with the following data:

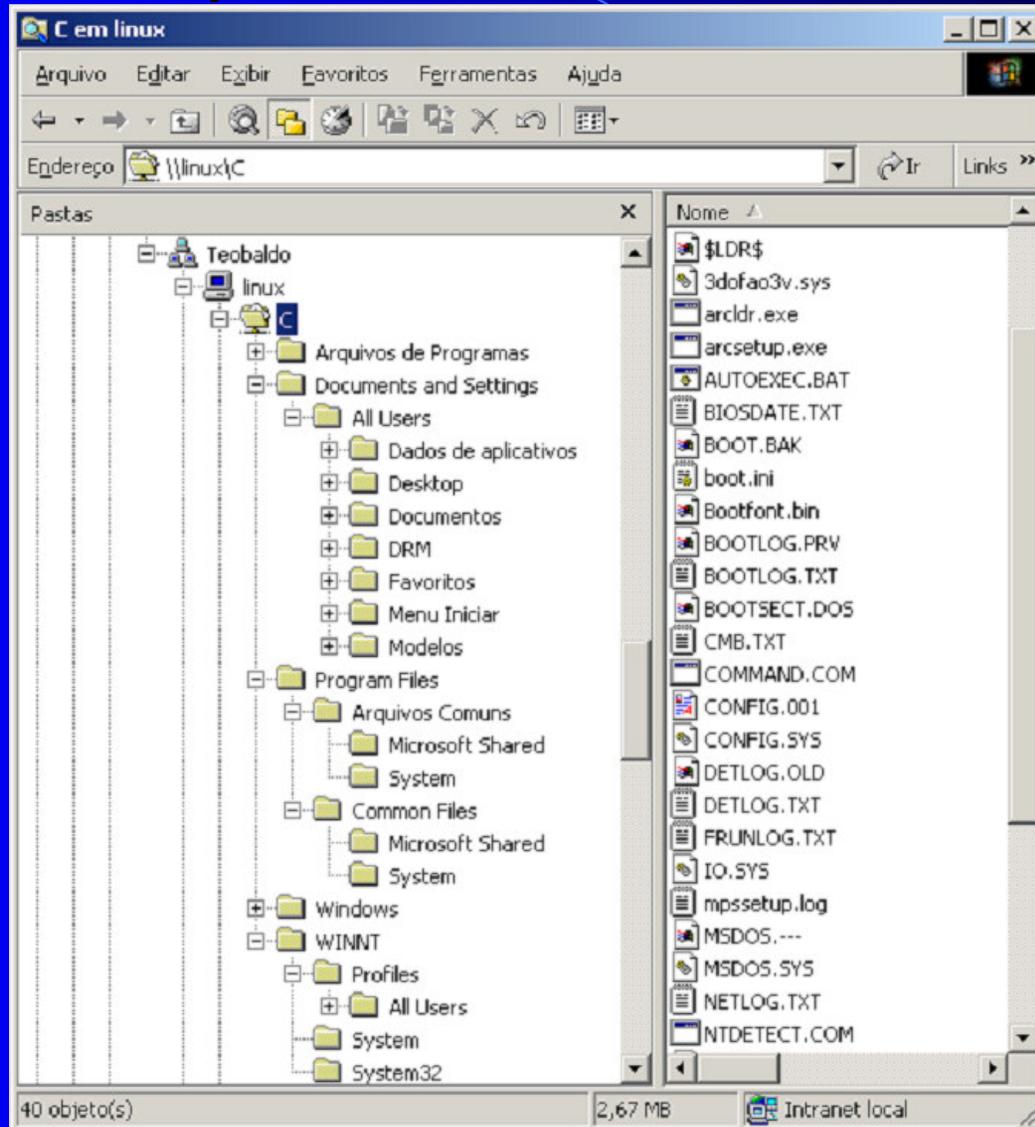
| # | Max. Origens | Max Dest. | Msgs. Dest. | Msgs. Or. Ext. | Interv. | Ação |
|---|--------------------------------|----------------------------------|---------------------------------|---------------------------------|---------------------------------------|------------------------------|
| 1 | <input type="text" value="5"/> | <input type="text" value="100"/> | <input type="text" value="30"/> | <input type="text" value="30"/> | <input type="text" value="02:00:00"/> | [Des.] [Alt] |
| # | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | [Incluir] |

At the bottom of the page, there are two links: [\[Topo\]](#) and [\[Voltar\]](#).

3.3 O Compartilhamento-Armadilha

- Criado através de um servidor CIFS (*Samba*);
- Permite acesso irrestrito a qualquer nome de compartilhamento solicitado pelas estações de trabalho da rede;
- Se algum agente malicioso for transmitido para o compartilhamento-armadilha, a estação correspondente será isolada da rede.

3.3.1 Arquivos e Pastas do Compartilhamento-Armadilha



3.4 O Isolamento

- Filtragem do tráfego gerado por estações de trabalho contaminadas impedindo que o agente malicioso se propague pela rede local.

3.4 O Isolamento

- A filtragem é feita nos servidores LIV e nos roteadores departamentais;
- Estações isoladas, ao tentarem navegar na Internet, receberão informações sobre a condição de isolamento;
- A relação das estações de trabalho contaminadas é replicada entre os servidores LIV parceiros da rede.

3.4.1 Fatores Determinantes do Isolamento

- Exame do tráfego de rede;
- Exame dos acessos ao servidor de correio;
- Exame dos anexos de correio;
- Exame dos acessos ao compartilhamento-armadilha;
- Solicitação de um servidor LIV parceiro;

3.4.2 Listagem de Estações Isoladas

LIV - Linux Integrated Viruswall - Microsoft Internet Explorer provided by SET/RN

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

LIV - Linux Integrated Viruswall

CONSULTAS INFORMAÇÕES ESTATÍSTICAS ADMINISTRAÇÃO LOGOUT (TEOBALDO)

ESTAÇÕES DE TRABALHO ISOLADAS

| # | ISOLAMENTO | | MOTIVO | | | | AÇÃO | |
|----|-------------------------------|---------------------|--------|--------------|-----------|--------|------|----------------------------|
| | IP | Data Isolamento | Remoto | Log Firewall | Log Email | Anexo | CIFS | |
| 1 | 10.19.19.29 | 2004-02-19 11:00:06 | | 5 | | | | Reintegrar |
| 2 | 10.26.0.181 | 2004-02-19 18:25:02 | | 3 | | | | Reintegrar |
| 3 | 10.5.0.200 | 2004-02-19 19:10:02 | | 2 | | | | Reintegrar |
| 4 | 10.5.0.33 | 2004-02-19 21:10:02 | | 2 | | | | Reintegrar |
| 5 | 10.5.0.52 | 2004-02-20 09:20:02 | | 2 | | | | Reintegrar |
| 6 | 10.19.51.35 | 2004-02-20 09:25:03 | | 5 | | | | Reintegrar |
| 7 | 10.5.0.17 | 2004-02-20 09:35:01 | | 2 | | | | Reintegrar |
| 8 | 10.160.19.11 | 2004-02-26 09:25:04 | | 5 | | | | Reintegrar |
| 9 | 10.184.101.1 | 2004-02-26 12:00:08 | | 5 | | | | Reintegrar |
| 10 | 10.18.0.161 | 2004-02-26 12:44:20 | | | | 651879 | | Reintegrar |
| 11 | 10.42.0.13 | 2004-02-26 14:00:26 | | | | 652784 | | Reintegrar |
| 12 | 10.9.8.133 | 2004-02-27 09:34:07 | | | | 665838 | | Reintegrar |
| 13 | 10.18.38.50 | 2004-02-27 09:49:59 | | | | 666069 | | Reintegrar |
| 14 | 10.9.3.39 | 2004-02-27 10:35:03 | | 5 | | | | Reintegrar |
| 15 | 10.20.1.30 | 2004-02-27 14:55:08 | | | 3 | | | Reintegrar |
| 16 | 10.19.0.54 | 2004-02-28 10:15:04 | 1 | | | | | Reintegrar |
| 17 | 10.196.16.40 | 2004-02-28 10:20:02 | | 5 | | | | Reintegrar |
| 18 | 10.20.7.3 | 2004-02-28 13:35:03 | | 4 | | | | Reintegrar |
| 19 | 10.126.15.218 | 2004-03-01 08:10:03 | | 5 | | | | Reintegrar |
| 20 | 10.126.15.204 | 2004-03-01 08:55:03 | | 5 | | | | Reintegrar |
| 21 | 10.126.15.205 | 2004-03-01 09:00:07 | | 5 | | | | Reintegrar |
| 22 | 10.126.15.6 | 2004-03-01 09:10:08 | | 5 | | | | Reintegrar |

3.4.3 Casos de Isolamento - *Blaster*

The screenshot shows a web browser window titled "LIV - Linux Integrated Viruswall - Microsoft Internet Explorer provided by SET/RN". The browser's menu bar includes "Arquivo", "Editar", "Exibir", "Favoritos", "Ferramentas", and "Ajuda". The main content area is titled "LIV - Linux Integrated Viruswall" and has a navigation bar with "CONSULTAS", "INFORMAÇÕES", "ESTATÍSTICAS", and "ADMINISTRAÇÃO".

The left sidebar contains four menu items: "CONSULTA MINHA ESTAÇÃO", "ESTAÇÕES ISOLADAS", "HISTÓRICO ISOLAMENTO", and "E-MAILS BANIDOS". The main content area displays the following information:

CONSULTA ESTAÇÃO - 10.40.0.97

A estação 10.40.0.97 foi isolada da rede em 2004-03-18 14:00:03. Para informações sobre o processo de isolamento e sobre como reintegrar o computador à rede, consulte a seção de [INFORMAÇÕES](#).

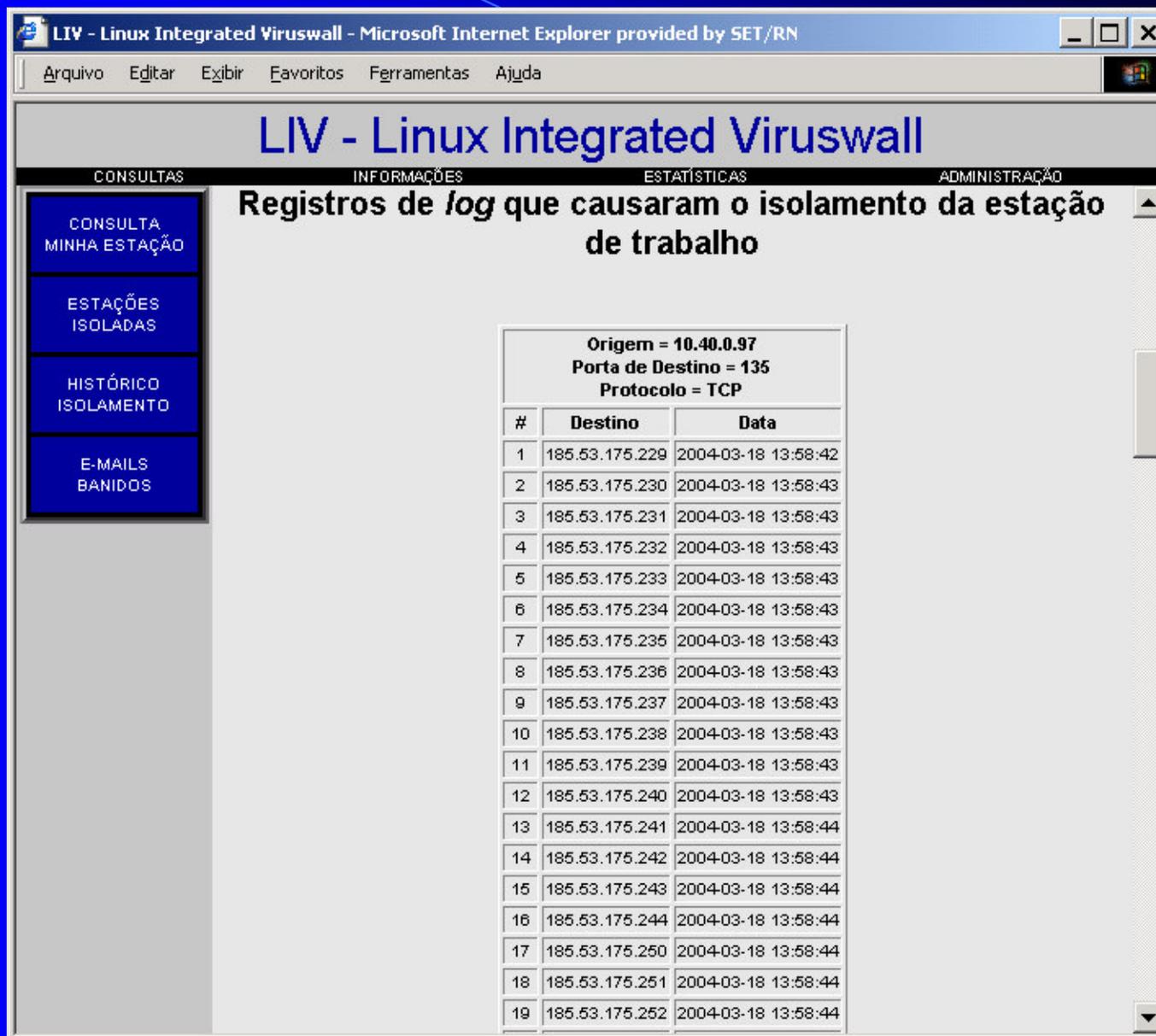
O motivo do isolamento foi o seguinte: Estação apresentou comportamento suspeito no tocante ao tráfego de rede gerado.

Esta estação de trabalho gerou um padrão de tráfego de rede que o administrador deste servidor LIV optou por considerar como suspeito. Este padrão pode indicar, por exemplo, uma contaminação por vírus, ou o funcionamento de algum outro tipo de programa malicioso. O padrão também pode ocorrer em função de configurações de rede incorretas ou atípicas (servidores WINS ou DNS informados erroneamente, máquinas desatualizadas, uso excessivo de recursos de rede, como impressoras ou unidades mapeadas, falta de contato com os controladores do domínio da máquina, etc.). Caso não seja encontrado vírus na máquina, verifique as configurações de rede, deixe na pasta "impressoras" apenas as realmente utilizadas, apague os atalhos desnecessários existentes em "Meus Locais de Rede", encerre as unidades mapeadas não utilizadas e feche os compartilhamentos de rede que não estão em uso.

Informações sobre a regra que causou o isolamento da estação de trabalho

| | |
|-----------|-----|
| PORTA | 135 |
| PROTOCOLO | TCP |
| ATRIBUTO | 3 |

3.4.4 Casos de Isolamento - *Blaster*



The screenshot shows a web browser window titled "LIV - Linux Integrated Viruswall - Microsoft Internet Explorer provided by SET/RN". The browser's menu bar includes "Arquivo", "Editar", "Exibir", "Favoritos", "Ferramentas", and "Ajuda". The main content area displays the "LIV - Linux Integrated Viruswall" interface with a navigation menu on the left and a central display area.

The navigation menu on the left includes the following options:

- CONSULTA MINHA ESTAÇÃO
- ESTAÇÕES ISOLADAS
- HISTÓRICO ISOLAMENTO
- E-MAILS BANIDOS

The central display area shows the "INFORMAÇÕES" tab selected, displaying the title "Registros de log que causaram o isolamento da estação de trabalho". Below the title, the following information is shown:

Origem = 10.40.0.97
Porta de Destino = 135
Protocolo = TCP

| # | Destino | Data |
|----|----------------|---------------------|
| 1 | 185.53.175.229 | 2004-03-18 13:58:42 |
| 2 | 185.53.175.230 | 2004-03-18 13:58:43 |
| 3 | 185.53.175.231 | 2004-03-18 13:58:43 |
| 4 | 185.53.175.232 | 2004-03-18 13:58:43 |
| 5 | 185.53.175.233 | 2004-03-18 13:58:43 |
| 6 | 185.53.175.234 | 2004-03-18 13:58:43 |
| 7 | 185.53.175.235 | 2004-03-18 13:58:43 |
| 8 | 185.53.175.236 | 2004-03-18 13:58:43 |
| 9 | 185.53.175.237 | 2004-03-18 13:58:43 |
| 10 | 185.53.175.238 | 2004-03-18 13:58:43 |
| 11 | 185.53.175.239 | 2004-03-18 13:58:43 |
| 12 | 185.53.175.240 | 2004-03-18 13:58:43 |
| 13 | 185.53.175.241 | 2004-03-18 13:58:44 |
| 14 | 185.53.175.242 | 2004-03-18 13:58:44 |
| 15 | 185.53.175.243 | 2004-03-18 13:58:44 |
| 16 | 185.53.175.244 | 2004-03-18 13:58:44 |
| 17 | 185.53.175.250 | 2004-03-18 13:58:44 |
| 18 | 185.53.175.251 | 2004-03-18 13:58:44 |
| 19 | 185.53.175.252 | 2004-03-18 13:58:44 |

3.4.5 Casos de Isolamento - BugBear

LIV - Linux Integrated Viruswall - Microsoft Internet Explorer provided by SET/RN

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

LIV - Linux Integrated Viruswall

CONSULTAS INFORMAÇÕES ESTATÍSTICAS ADMINISTRAÇÃO LOGOUT (TEOBALDO)

CONSULTA ESTAÇÃO - 10.160.0.18

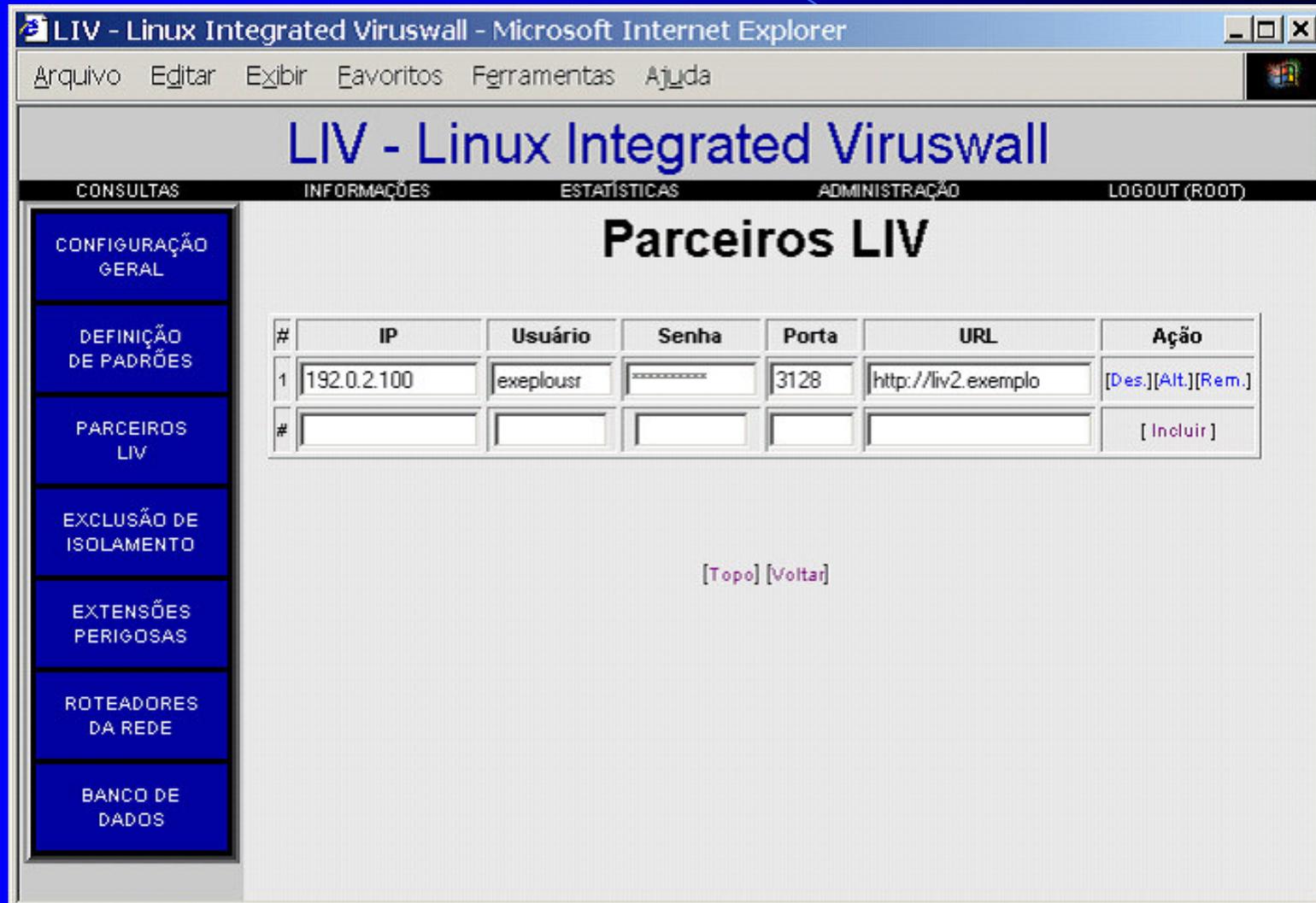
A estação 10.160.0.18 foi isolada da rede em 2004-02-04 08:23:55. Para informações sobre o processo de isolamento e sobre como reintegrar o computador à rede, consulte a seção de [INFORMAÇÕES](#).

O motivo do isolamento foi o seguinte: Estação transmitiu vírus através de compartilhamento de rede em 2004-02-04 08:23:55.

Esta estação de trabalho transmitiu o vírus Worm/BugBear.1 virus para o compartilhamento armadilha do servidor LIV. Este compartilhamento tem como objetivo identificar as estações contaminadas com vírus capazes de propagar-se através da rede local, contaminando as máquinas através de compartilhamentos de rede criados sem segurança. Esta estação de trabalho está, portanto, infectada.

[Topo] [Voltar]

3.4.6 Replicação entre Servidores LIV



The screenshot shows the web interface of the Linux Integrated Viruswall (LIV) system. The browser window title is "LIV - Linux Integrated Viruswall - Microsoft Internet Explorer". The interface has a menu bar with "Arquivo", "Editar", "Exibir", "Favoritos", "Ferramentas", and "Ajuda". Below the menu bar, the title "LIV - Linux Integrated Viruswall" is displayed. A navigation bar contains "CONSULTAS", "INFORMAÇÕES", "ESTATÍSTICAS", "ADMINISTRAÇÃO", and "LOGOUT (ROOT)". The main content area is titled "Parceiros LIV" and contains a table with columns: "#", "IP", "Usuário", "Senha", "Porta", "URL", and "Ação". The table has one row with the following data: "# 1", "IP 192.0.2.100", "Usuário exeploustr", "Senha [masked]", "Porta 3128", "URL http://liv2.exemplo", and "Ação [Des.][Alt.][Rem.]". Below the table, there is a row with empty input fields for "#", "IP", "Usuário", "Senha", "Porta", "URL", and "Ação", with a "[Incluir]" button. At the bottom of the page, there are links for "[Topo]" and "[Voltar]". On the left side, there is a vertical menu with buttons for "CONFIGURAÇÃO GERAL", "DEFINIÇÃO DE PADRÕES", "PARCEIROS LIV", "EXCLUSÃO DE ISOLAMENTO", "EXTENSÕES PERIGOSAS", "ROTEADORES DA REDE", and "BANCO DE DADOS".

| # | IP | Usuário | Senha | Porta | URL | Ação |
|---|-------------|------------|----------|-------|---------------------|--------------------|
| 1 | 192.0.2.100 | exeploustr | [masked] | 3128 | http://liv2.exemplo | [Des.][Alt.][Rem.] |
| # | | | | | | [Incluir] |

3.4.7 Isolamento nos Roteadores Departamentais



The screenshot displays the LIV - Linux Integrated Viruswall web interface. The browser window title is "LIV - Linux Integrated Viruswall - Microsoft Internet Explorer provided by SET/RN". The interface has a menu bar with "CONSULTAS", "INFORMAÇÕES", "ESTATÍSTICAS", "ADMINISTRAÇÃO", and "LOGOUT (TEOBALDO)". A left sidebar contains navigation options: "CONFIGURAÇÃO GERAL", "DEFINIÇÃO DE PADRÕES", "PARCEIROS LIV", "EXCLUSÃO DE ISOLAMENTO", "EXTENSÕES PERIGOSAS", "ROTEADORES DA REDE", and "BANCO DE DADOS". The main content area is titled "Roteadores da Rede Protegida" and contains a table with the following data:

| # | Roteador | Rede | CIDR | Ação |
|----|-----------|------------|------|--------------------|
| 1 | 10.1.0.10 | 10.6.4.0 | 24 | [Alterar][Remover] |
| 2 | 10.1.0.10 | 10.7.5.0 | 24 | [Alterar][Remover] |
| 3 | 10.1.0.10 | 10.19.10.0 | 24 | [Alterar][Remover] |
| 4 | 10.1.0.10 | 10.20.3.0 | 24 | [Alterar][Remover] |
| 5 | 10.1.0.10 | 10.23.1.0 | 24 | [Alterar][Remover] |
| 6 | 10.1.0.10 | 10.28.0.0 | 24 | [Alterar][Remover] |
| 7 | 10.1.0.10 | 10.29.0.0 | 24 | [Alterar][Remover] |
| 8 | 10.1.0.10 | 10.30.0.0 | 24 | [Alterar][Remover] |
| 9 | 10.1.0.10 | 10.31.0.0 | 24 | [Alterar][Remover] |
| 10 | 10.1.0.10 | 10.34.0.0 | 24 | [Alterar][Remover] |
| 11 | 10.1.0.10 | 10.37.0.0 | 24 | [Alterar][Remover] |
| 12 | 10.1.0.10 | 10.38.0.0 | 24 | [Alterar][Remover] |
| 13 | 10.1.0.10 | 10.39.0.0 | 24 | [Alterar][Remover] |

- 4 -

Resultados Obtidos

4.1 A Rede Protegida pelo LIV

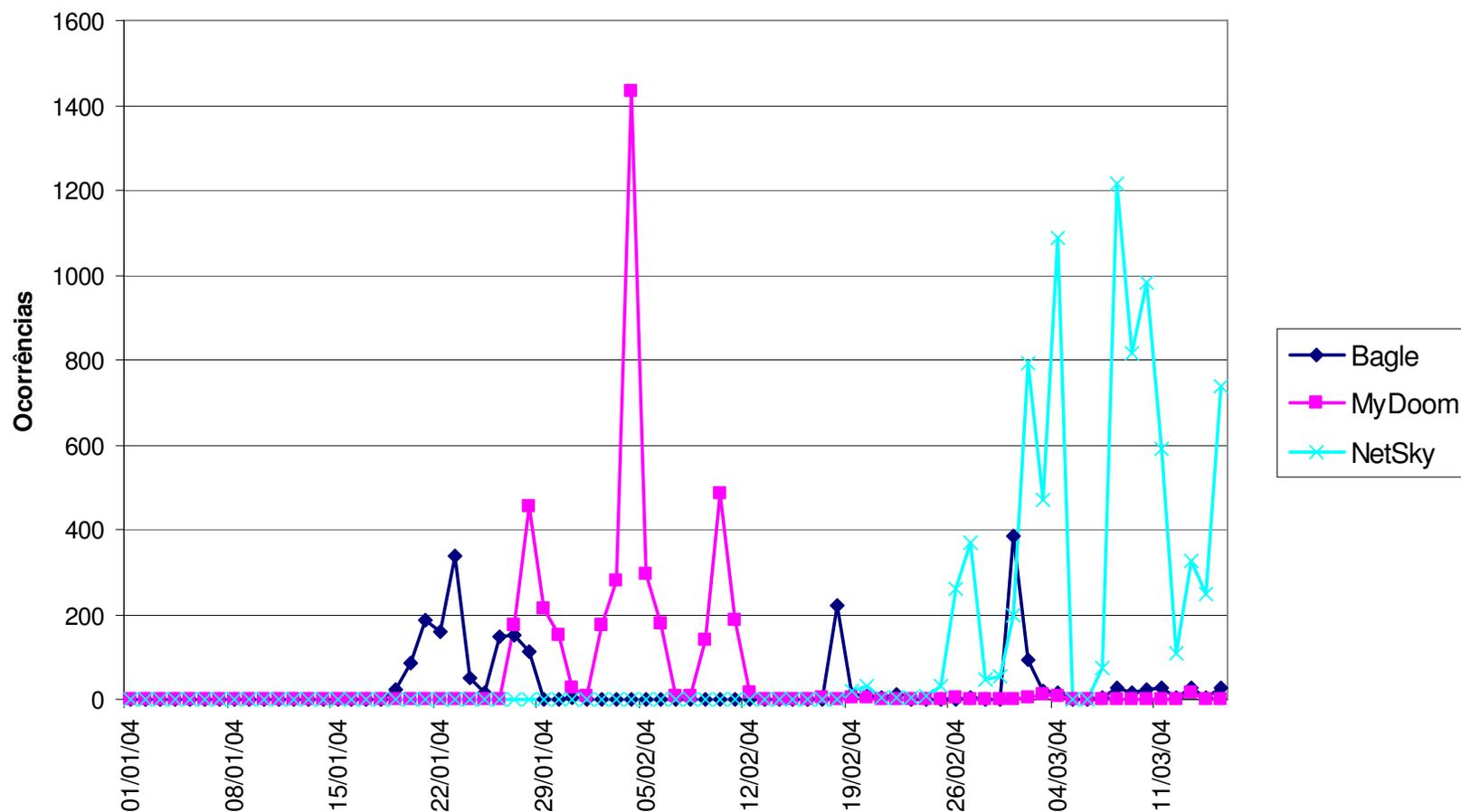
- 6.000 estações de trabalho Windows;
- 180 pontos de presença no Estado do RN;
- Interconexão com a Internet por canal de 6 Mbps;
- Administração centralizada em Natal/RN;
- LIV implantado em janeiro de 2004.

4.2 O Filtro SMTP

| | |
|---|-----------|
| Mensagens Roteadas pelo LIV (Período: 08/01/04 – 15/03/04) | 1.051.528 |
| Média Diária de Mensagens | 15.463 |
| % Correios Originados na Intranet | 62,0 % |
| Anexos Examinados | 248.367 |
| Anexos Infectados | 19.455 |
| % Anexos Infectados | 7,83 % |

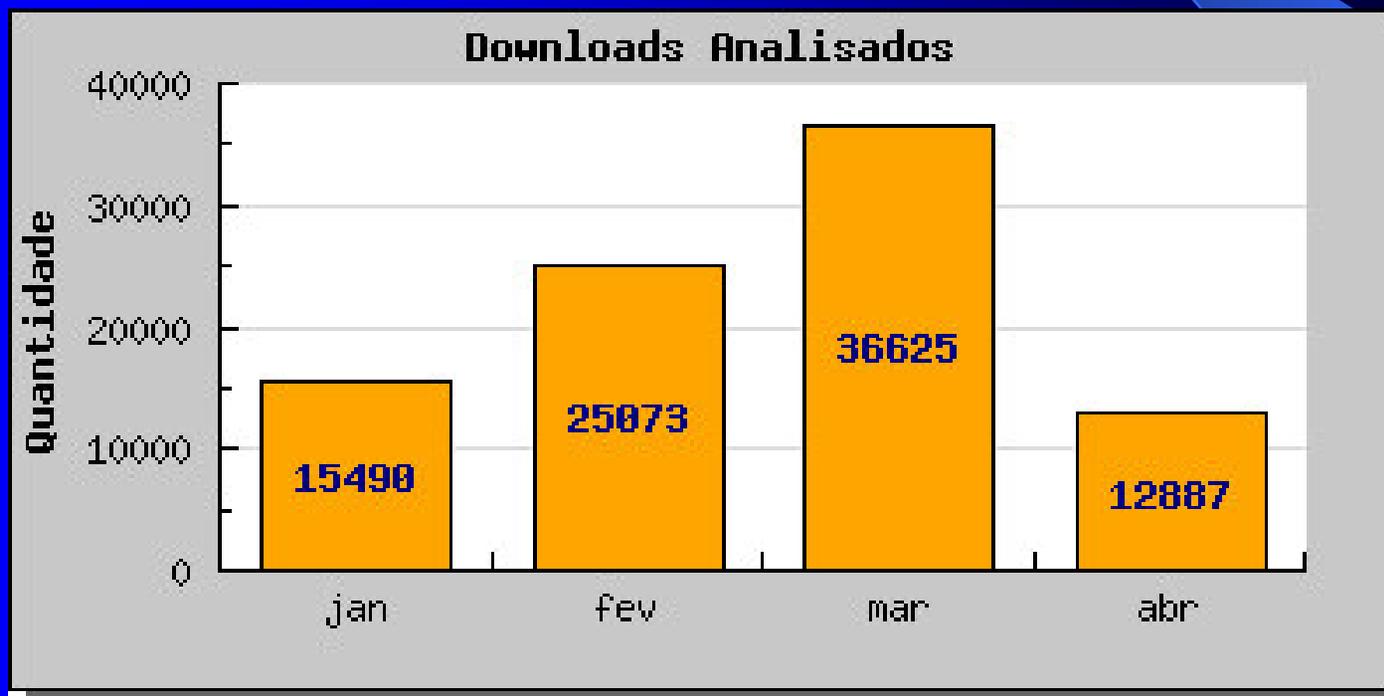
4.2.1 Infestações Contidas pelo Filtro SMTP do LIV

Principais Infestações Contidas pelo Filtro SMTP do LIV por Dia



4.3 Exame dos *Downloads*

- *Downloads* analisados de 08/01/04 a 16/04/04: 90.075 (901 por dia). 50 Infectados (0,05 %).



4.4 O Compartilhamento-armadilha

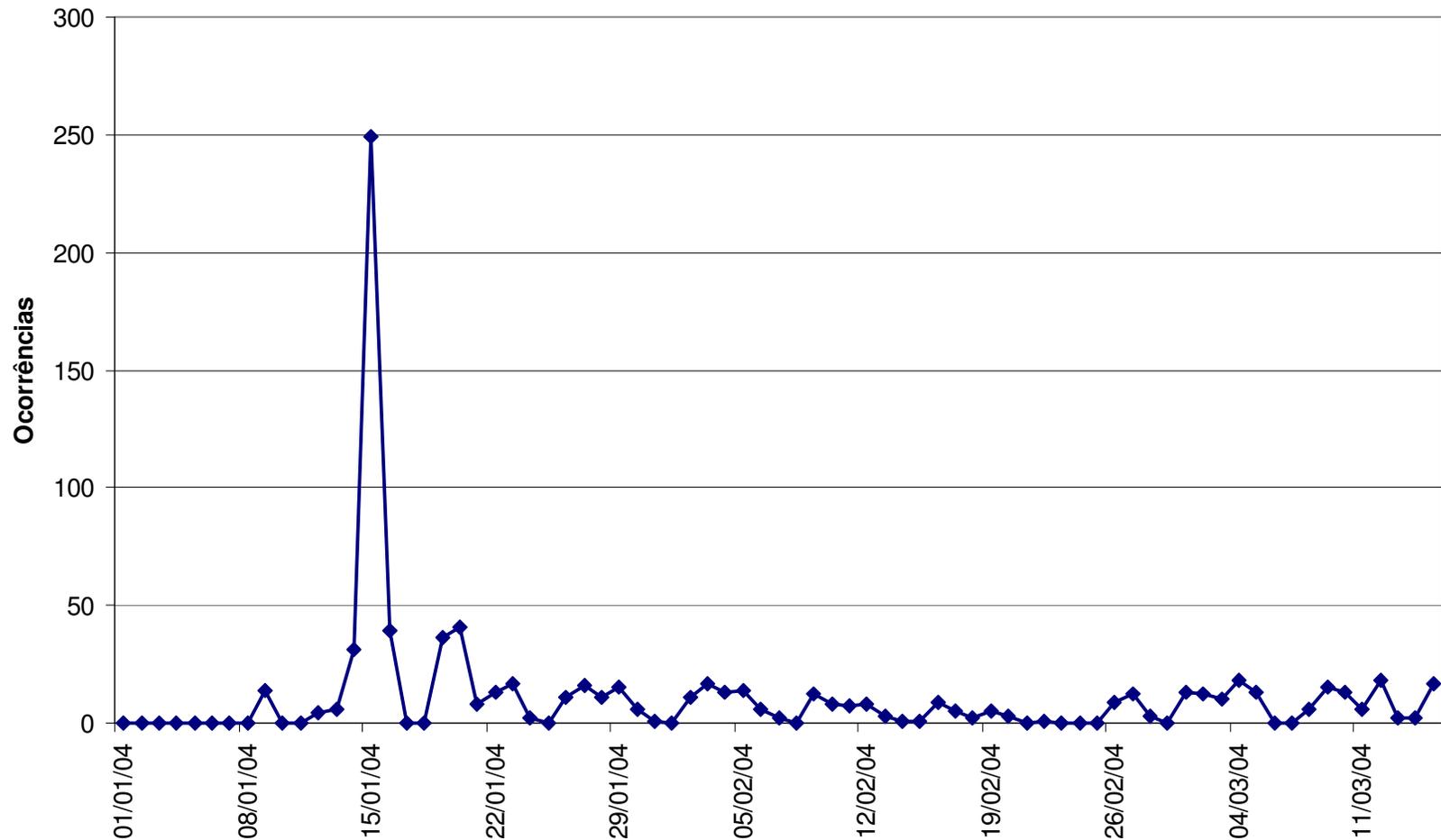
- 132 acessos;
- 27 dos acessos, realizados por 4 estações, resultaram na inserção de código malicioso no compartilhamento;
- Agentes Maliciosos:
 - BugBear.1
 - Bugbear.B
 - Funlove

4.4.1 Atuação do Compartilhamento-armadilha

- Apr 16 17:21:11 LIV [3929]: ALERT: [W32/Funlove virus] /usr/local/liv/armadilha/Arquivos de Programas/Windows Media Player/logagent.exe <<< Contains code of the Windows virus W32/Funlove (removeable)
- Apr 16 17:21:11 LIV [4022]: ALERT: [W32/Funlove virus] /usr/local/liv/armadilha/Arquivos de Programas/Windows Media Player/dlimport.exe <<< Contains code of the Windows virus W32/Funlove (removeable)
- Apr 16 17:21:11 LIV [4025]: ALERT: [W32/Funlove virus] /usr/local/liv/armadilha/Arquivos de Programas/Windows Media Player/setup_wm.exe <<< Contains code of the Windows virus W32/Funlove (removeable)

4.5 Isolamentos Realizados

Isolamentos por Dia

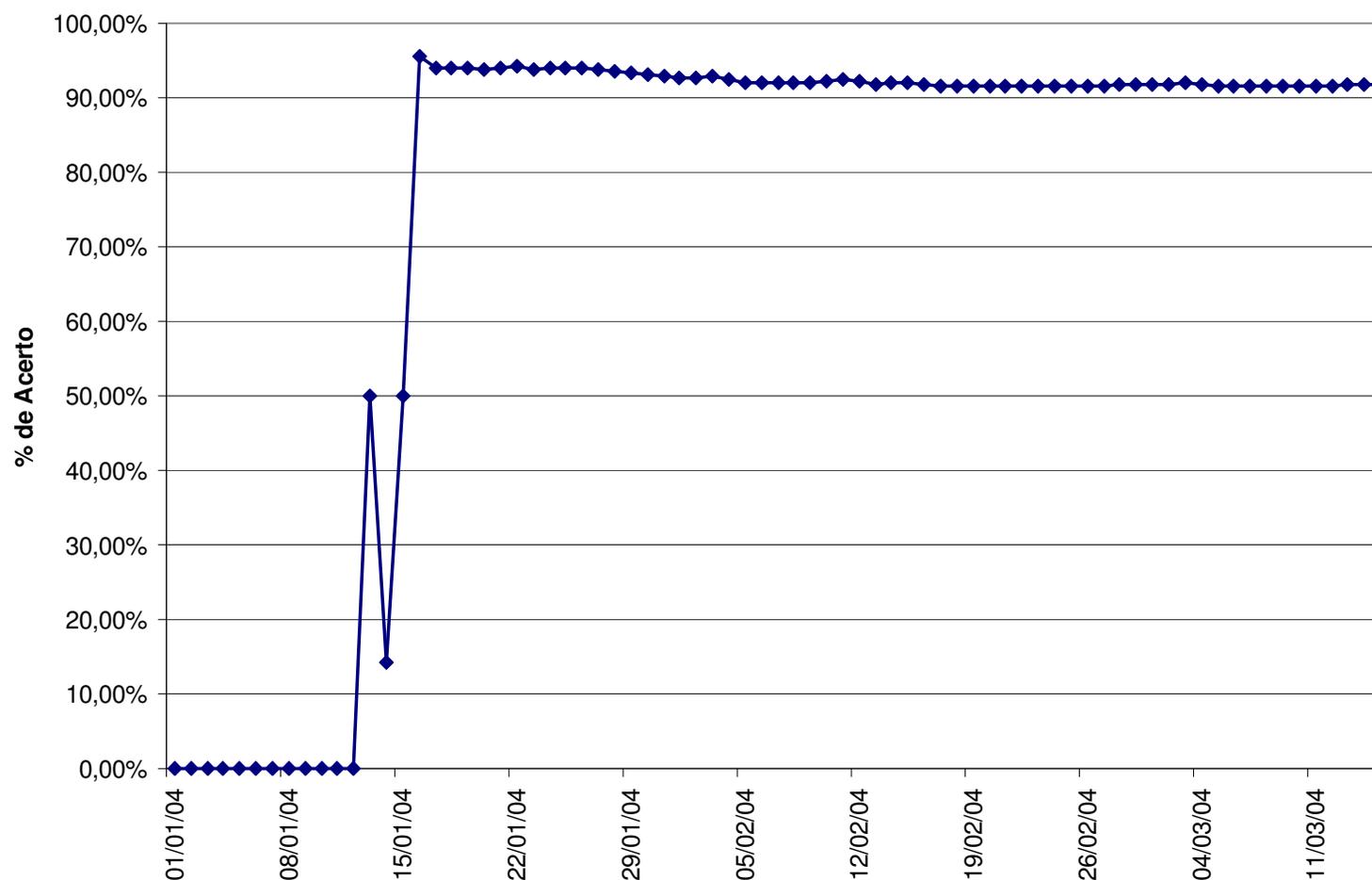


4.5.1 Razões para o Isolamento das Estações

| | |
|---|---------|
| Tráfego de Rede Suspeito | 68,45 % |
| Envio de Anexo Infectado | 26,88 % |
| Acesso Suspeito ao Servidor de Correio | 4,32 % |
| Transmissão de Agente Malicioso ao Compartilhamento Armadilha | 0,35 % |

4.5.2 Taxa de Acerto no Isolamento

Evolução Diária do Percentual de Estações Comprovadamente Infectadas sobre o Total dos Isolamentos Realizados pelo LIV



- 5 -

Conclusões

5 - CONCLUSÕES

- O LIV é um Sistema antivírus proposto para o ambiente Linux visando à proteção de redes locais Windows.
- É reativo e pró-ativo.
- Integra servidores **CIFS**, **SMTP**, **HTTP**, *proxy*, um servidor de banco de dados e uma *firewall*.

5 – CONCLUSÕES (cont.)

- Protege contra códigos maliciosos conhecidos e contra dados considerados suspeitos.
- É capaz de detectar a contaminação de estações de trabalho através da análise do tráfego de rede.
- Interage com os usuários e com o administrador via **WEB**.

CONTATOS E AGRADECIMENTOS

Teobaldo Medeiros

CEFET/RN:

E-mail: teobaldo@cefetrn.br

GOVERNO DO ESTADO DO RIO GRANDE DO NORTE,
SECRETARIA DE ESTADO DE TRIBUTAÇÃO:

E-mail: teobaldo@set.rn.gov.br

Paulo Motta

UFRN

E-mail: pmotta@dca.ufrn.br