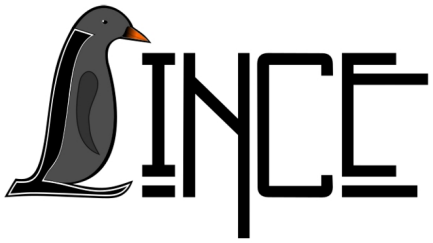
Website



Facebook

Tutorial para Remover Vírus Manoel.doc

Autor(es)
Lucas Fank

Colaborador(es)

Orientador(es)
Everton W. Bocca

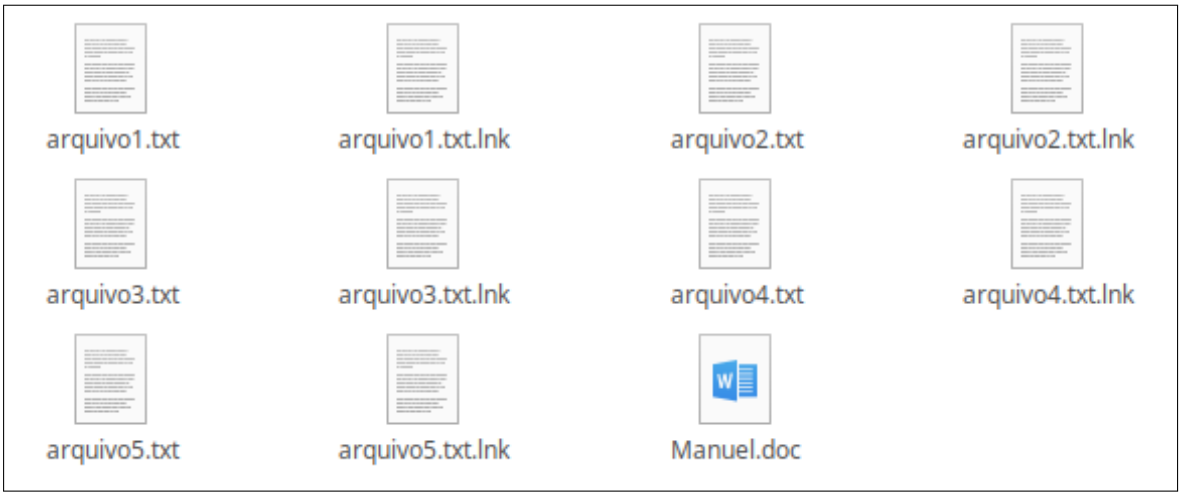
22 de julho de 2020

Sumário

1 Introdução

O **Manuel.doc** ou **Manoel.doc** é um vírus que infecta o dispositivo e converte arquivos e pastas em atalhos. Isso impede que o usuário abra qualquer anexo, e muitas vezes leva à formatação sem necessidade da unidade removível, pois os arquivos ainda estão lá. A visualização do Pen Drive normalmente é parecida com a da Figura 1.1, onde existem os arquivos originais e os arquivos com o mesmo nome com a extensão de arquivos `.lnk`, esta que representa os atalhos. Também na Figura 1.1 é possível visualizar o arquivo `Manuel.doc`.

Figura 1.1 – Exemplo de Pen Drive infectado



Fonte: Acervo da Unidade

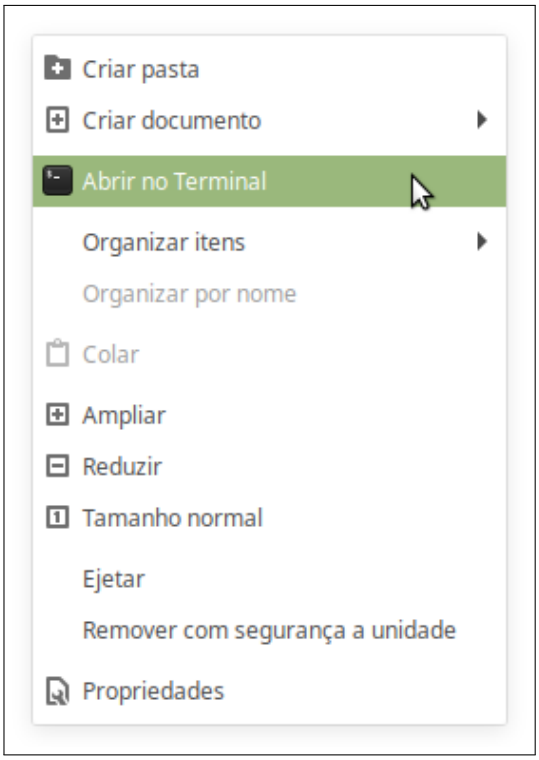
2 Removendo Vírus

2.1 Utilizando distribuição GNU/Linux

2.1.1 Removendo os atalhos

Para remover os arquivos com a extensão `.lnk`, primeiramente abra o Pen Drive em um computador com GNU/Linux, em seguida acesse o Pen Drive, onde clique com o botão direito do mouse e escolha a opção `Abrir no Terminal`, como mostra a Figura 2.1.

Figura 2.1 – Abrindo o Pen Drive no Terminal



Fonte: Acervo da Unidade

Agora já no Terminal digite o comando a seguir, como mostra a Figura 2.2.

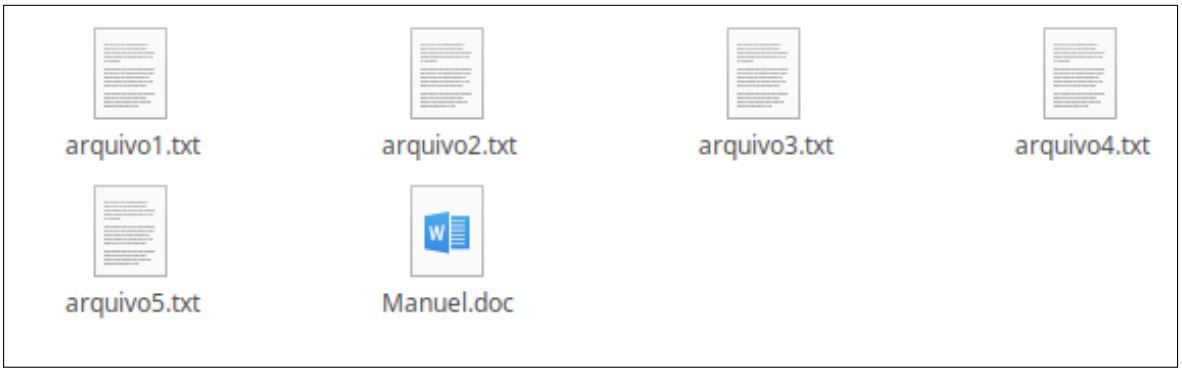
```
$ sudo rm -Rf *.lnk
```

Figura 2.2 – Removendo arquivos .lnk pelo Terminal

Fonte: Acervo da Unidade

Após remover os arquivos com a extensão `*.lnk`, somente deverão estar no Pen Drive os arquivos originais e o arquivo `Manuel.doc`, como mostra a Figura 2.3.

Figura 2.3 – Exemplo de Pen Drive sem os atalhos, mas com o Manuel.doc



Fonte: Acervo da Unidade

Abaixo será descrito como cada uma das opções do comando funcionam, para melhor entendimento.

1. **sudo -** O comando dever ser executado como superusuário para que o comando possa executar livremente, sem restrições.

2. **rm -** O comando efetivo a ser executado é o `rm`, pois no terminal GNU/Linux, é utilizado para remover arquivos e/ou diretórios, neste caso, para que ele seja efetivo na remoção dos arquivos indesejados ele precisa dos demais complementos do comando.

3. **-Rf -** Parâmetros adicionados ao comando após o sinal de `-`. O parâmetro `R` indica que comando será recursivo, ou seja, ele irá remover os arquivos a partir da raiz até todos os subdiretórios e o `f`, forçado, que garante que ele poderá remover sem qualquer restrição imposta por permissões.

4. ***.lnk -** Especifica que o comando deverá excluir, `*`, todos os arquivos com a extensão `.lnk`.

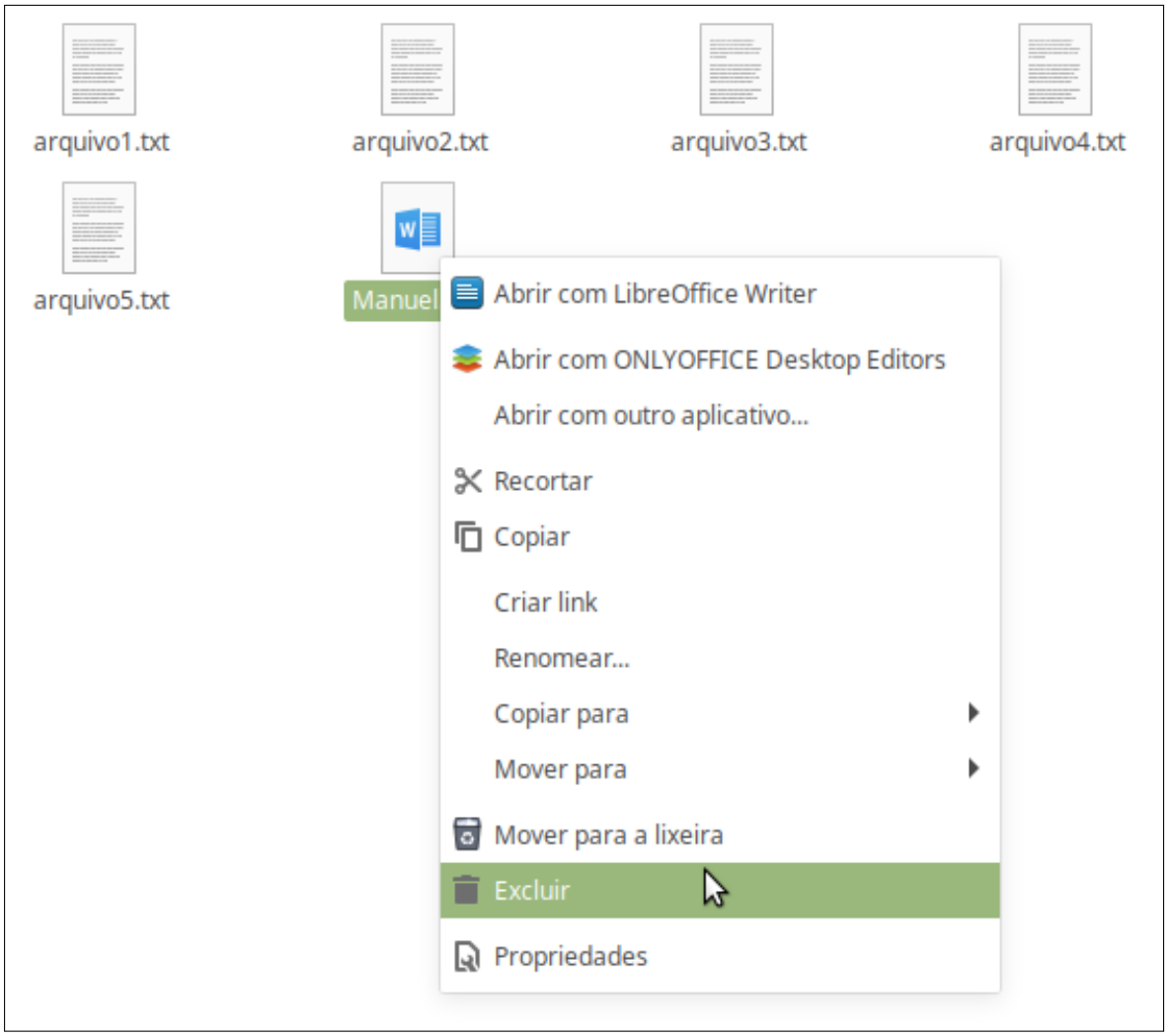
2.1.2 Remover o Manuel.doc

Remover os arquivos de atalho, com a extensão `*.lnk`, não garante uma limpeza completa no Pen Drive, já que o documento `Manuel.doc` é composto por um `script` que é executado automaticamente e infecta o computador onde o Pen Drive foi conectado.

Para remover o arquivo `Manuel.doc`, pode-se usar a interface gráfica, clicando com o botão direito sobre o arquivo e após em `Excluir`, como mostra a Figura 2.4. Também é possível remover este arquivo pelo Terminal, com a execução do comando a seguir em um Terminal que esteja com o Pen Drive aberto, como mostra a Figura 2.5.

```
$ sudo rm Manuel.doc
```

Figura 2.4 – Removendo o arquivo Manuel.doc pela Interface Gráfica



Fonte: Acervo da Unidade

Figura 2.5 – Removendo o arquivo Manuel.doc pelo Terminal

```
pccli@carlos-pc /media/pccli/867C16C27C16AD45 $ sudo rm -f Manuel.doc
```

Fonte: Acervo da Unidade

Com a remoção do arquivo `Manuel.doc` e dos arquivos com a extensão `.lnk` o Pen Drive está livre do vírus, como mostra a Figura 2.6.

Figura 2.6 – Exemplo de Pen Drive sem os atalhos e sem o Manuel.doc

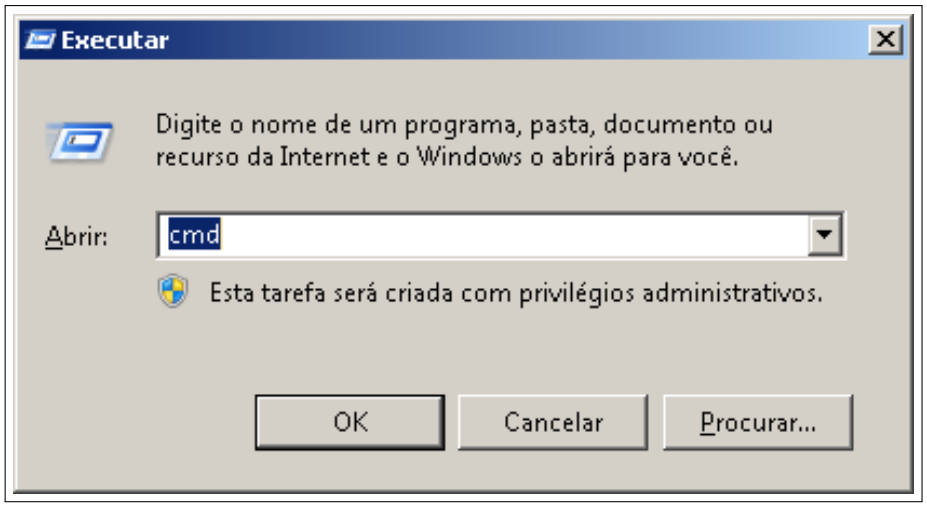
Fonte: Acervo da Unidade

2.1.3 Mostrar Pastas no Windows

Após realizar a limpeza do Pen Drive é preciso realizar um procedimento no Windows. Para isto, basta conectar o Pen Drive em um computador com o Sistema Operacional Windows, após a limpeza no GNU/Linux, e executar um comando no Prompt de Comando, ao conectar o Pen Drive mo Windows após a limpeza, todos os arquivos e diretórios estarão ocultos.

Para executar o comando a seguir pesquise `cmd` no Menu Iniciar ou utilize o atalho do teclado **Windows + R** para abrir o `Executar` e insira o comando `cmd`, como na Figura 2.7.

Figura 2.7 – Abrindo o Prompt de Comando



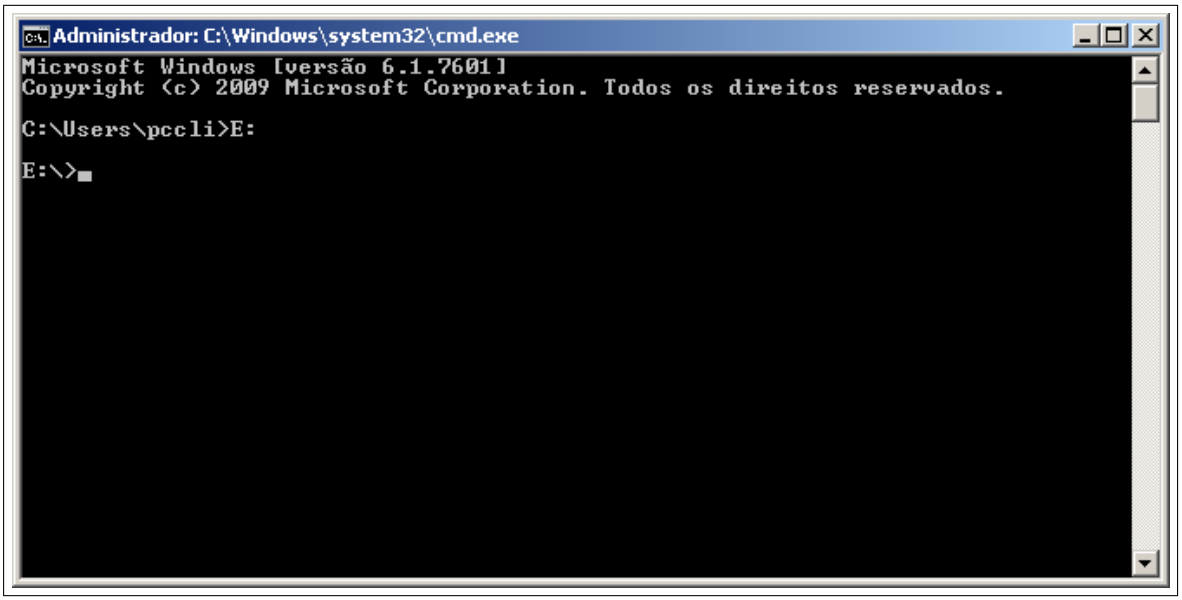
Fonte: Acervo da Unidade

Primeiramente navegue até a unidade do Pen Drive, para isso digite a letra da unidade correspondente, como mostra o exemplo do comando a seguir e da Figura 2.8.

```
X:
```

Obs. OBS: Altere a letra `X` pela letra definida para o seu Pen Drive

Figura 2.8 – Navegando até o Pen Drive no Prompt de Comando

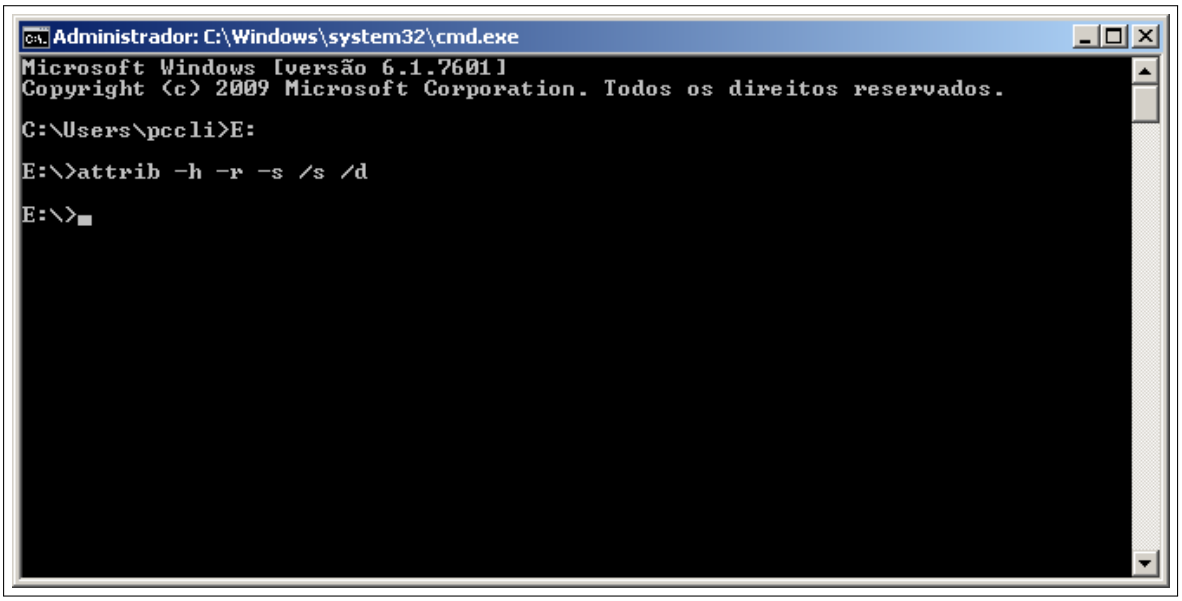


Fonte: Acervo da Unidade

Já dentro do Pen Drive digite o comando a seguir, que irá garantir que os arquivos e diretórios estejam visíveis no Windows, como mostra a Figura 2.9.

```
attrib -h -r -s /s /d
```

Figura 2.9 – Executando o comando attrib no Prompt de Comando



Fonte: Acervo da Unidade

Abaixo será descrito como cada uma das opções do comando funcionam, para melhor entendimento.

1. **attrib -** Este comando exibe, define ou remove os atributos de arquivos ou diretórios. Se usado sem parâmetros, ele exibe os atributos de todos os arquivos no diretório atual.

Este é o comando efetivamente executado, que precisa dos parâmetros e opções a seguir para atender o nosso objetivo, de remover o atributo `Oculto` dos arquivos.

2. **-r -** Parâmetros que remove o atributo de `Somente Leitura` de arquivos e diretórios.

3. **-s -** Parâmetros que remove o atributo de `Oculto` de arquivos e diretórios.

4. **-h -** Parâmetros que remove o atributo de `Oculto` de arquivos e diretórios.

5. **/s -** Parâmetros que aplica o comando e qualquer parâmetro aos arquivos correspondentes no diretório atual e em todos os seus subdiretórios.

6. **/d -** Parâmetros que aplica o comando e qualquer parâmetro aos diretórios. Somente é possível usar o `/d` com o `/s`.