Análise de malwares - comandos iniciais

Quando possuímos um artefato malicioso em que precisamos fazer uma análise existem alguns comandos básicos que nós utilizamos para entender um pouco da estrutura deste artefato.

O primeiro deles é o comando file, o comando file nos mostra a extensão de um arquivo, e não se enganem, não é porque um arquivo possui um ".pdf" que ele realmente se trata de um pdf, muitos dos que criam artefatos maliciosos usam um extensão falsa para não levantar suspeitas, usando o comando file nós podemos ver a verdadeira extensão de um arquivo e também para qual tipo de sistema operacional ele foi desenvolvido, vejam a estrutura do comando:

```
file -a nome_do_arquivo
```

A flag -a usada neste exemplo faz com que o file nos traga a informação de forma mais objetiva, basicamente só aquilo que é mais "útil", você pode usar a flag -i e ele trará algumas informações a mais. Para saber mais sobre o comando file use `man file`.

Temos também o comando strings, o comando strings pega todas as strings de um arquivo e exibe ela na tela ou joga para dentro de outro arquivo, usar este comando é uma boa ideia pois sua análise se torna mais segura ao não executar o artefato.

```
strings nome_do_arquivo
```

Ou

```
strings nome_do_arquivo > teste.txt
```

- O segundo comando manda as strings do arquivo escolhido para um arquivo .txt (você decide o nome).

O próximo comando é o hexdump, não tem muito segredo, basta digitar hexdump e o nome do arquivo como todos os outros comandos anteriores e será exibido para você todo o hexadecimal do arquivo escolhido.

```
hexdump nome_do_arquivo
```

- É interessante destacar que para saber mais sobre qualquer um desses comandos você pode usar o comando man seguido do nome do comando para ler o manual do comando.

jcesar_n

JulioCesarNSM

Obrigado!