Terceiro Trabalho de Segurança

Lucas Rodrigues Teixeira Nunes[1]
DRE: 113202670

[1]Departamento de Ciência da Computação -
Instituto de Matemática -
Universidade Federal do Rio de Janeiro

1. Objetivo

O objetivo do trabalho é desenvolver um vírus que seja o mais malicioso possível e explicar cada passo do seu funcionamento.

2. Ideia do vírus

Pela dificuldade em ter ideias de como infectar outros arquivos e o que fazer após infectá-los, optei por me basear no vírus mostrado em sala de aula, devido à minha falta de conhecimento das principais vulnerabilidades de um sistema Linux. Porém, embora seja um vírus simples, causa danos muito graves ao sistema onde foi executado, uma vez que deleta o diretório `\boot`. Com isso, ao ser desligado ou reiniciado, a máquina não conseguirá encontrar os arquivos necessários para a inicialização e o sistema será inutilizado.

Para deletar o diretório em questão, são necessários privilégios de root, portanto ao simular o funcionamento do vírus, é necessário estar logado como o usuário root.

3. Funcionamento do vírus

Como dito na seção 2, o vírus foi baseado no código mostrado em sala de aula, com algumas modificações na forma como ele busca arquivos para serem infectados. Primeiramente, ele procura outros arquivos `.py` no mesmo diretório onde ele se encontra utilizando a função `search_files`. Caso não hajam apenas arquivos dentro do diretório, a busca é estendida para as pastas seguintes, até infectar todos os arquivos `.py` nos diretórios subsequentes. Caso um arquivo passível de infecção seja encontrado, seu `path` é acrescentado à lista de arquivos a serem infectados. Também é feita uma checagem para determinar se o arquivo sendo analisado no momento se trata do próprio arquivo do vírus, para evitar que ele se replique dentro do próprio código.

Quando todos os arquivos forem encontrados, na função `infect_files`, o próprio arquivo se abre para leitura e copia seu código para cada arquivo encontrado pela função `search_files`.

Por fim, a função `destroy` utiliza o método `os.system` para executar uma call na linha de comando do Linux, e a call escolhida foi `rm -r \boot`, para que o diretório de boot seja deletado e todos os outros diretórios e arquivos que possam estar contidos nele.

Ao tentar rebootar a máquina virtual, o seguinte erro foi apresentado: "`FATAL ERROR: No booting medium found!`"

4. Conclusão

Com a realização deste trabalho, ficou ainda mais claro que não são necessários grandes ferramentas ou conhecimentos técnicos para criar um vírus bastante malicioso. Embora a aplicabilidade real deste vírus seja praticamente nula, a falta de atenção do usuário de um sistema qualquer pode levá-lo a executar arquivos que podem ser extremamente prejudiciais tanto à máquina em si, quanto à segurança dos dados do usuário em questão.