TAG- Segurança Ofensiva 1

Nome: Mariane Ferreira

Escolha de Ataque: Malware (um spyware).

Tipo de Malware: Keylogger

O que é um Keylogger?

É um spyware que tem como objetivo capturar tudo que for digitado no teclado. Ele identifica quais teclas foram pressionadas e escreve em um arquivo texto. A leitura desse arquivo de texto pelo atacante, pode ser feita manualmente (indo ao computador recuperar o arquivo) ou implementando um código na qual envia o arquivo para algum lugar em que o atacante tem acesso online, em uma determinada frequência de tempo.

Para que serve um Keylogger?

A princípio, serve para roubar dados digitados pelo usuários, desde conversas pessoais, senhas, dados de cartão de crédito, dados pessoais como nome e CPF. Quando não são utilizados para fins anti-éticos, serve para guardar tudo que uma pessoa digita para ela mesma recuperar depois, como por exemplo, pessoas que digitam textos muito longos durante muito tempo. O keylogger não se limita apenas no mundo do software, há dispositivos de hardware que pode ser espetados no computador (em formato de pen driver) e capturar tudo que o usuário digitar.

Caso de uso antiético de um keylogger:

Um amigo meu usa windows e nao entende muito de computadores. Porém, ele faz bastante compras online. Eu instalaria um keylogger no computador dele para roubar os logins nos sites de compra e, de quebra, roubaria os dados de cartão de crédito, já que esses dados não são digitados via teclado virtual.

Caso de uso ético de um keylogger:

Eu gostaria de registrar tudo que eu digito para futuras consultas, e o arquivo na qual esté sendo gravado não sairia do meu computador.

Como evitar ser roubado por um keylogger?

Usando o teclado virtual, que faz a comunicação direto com o sistema operacional. Você só poderia ser roubado se tivesse algum malware que printasse a sua tela a uma certa frequência de tempo ou que pegasse os dados do campo que você está preenchendo

Sobre a implementação do meu Keylogger:

Ele é um arquivo .exe escrito em C++. Escolhi implementar para Windows porque é o sistema operacional mais suscetível a ataques (e porque eu odeio o windows).

Se você resolver executá-lo, execute com permissão do administrador, pois o arquivo texto fica na pasta Windows do disco C: e se chama setup.txt.

Ele captura todas as teclas alfanuméricas do teclado, e teclas como capslock, backspace e os números do teclado numlock são escritos no arquivo com seus respectivos nomes, Exemplo: ("capslock is pressed").

Para matar o keylogger, basta encerrar o processo "keylogger" no gerenciador de arquivos e apagar o arquivo "setup" da pasta Windows

Problemas encontrados:

1. Não sei programar muito bem, então não consegui colocar todos os caracteres gravados no arquivo em uma linha só, tive que dar quebra de linha para cada ação do teclado porque ele simplesmente não escrevia sem fazer isso.
2. Esconder a tela de prompt quando inicia o executável, mas foi resolvido.
3. O keylogger não captura todos os caracteres (como os especiais por exemplo).
4. Os números do numlock não eram entendido como números, e sim como letras, ao apertar o "1", a letra "a" é escrita no arquivo, "resolvi" o problema identificando as teclas do numlock (agora quando você aperta o "1" sai a letra "a" e em seguida "numlock 1".
5. O antivírus tentou deletar o meu trabalho.