

Forum: [Hack Forums](#)

Thread: [Parameter injection in .exe \(C++\)](#)

SIM-5195853 - June 5, 2022, 5:22 pm

The parameters injection at the end of the file is very useful, for example, in trojans creation like keyloggers or rats.

We create two projects (I'm in Visual Studio), one for the stub and the other one for the builder. The builder will inject the parameters into the stub, and the stub will read the injected message from the builder.

Stub source code:

```
Code #include <fstream>
#include <iostream>
#include <Windows.h>
```

```
using namespace std;
```

```
#define STUB_SIZE 232448 //Compiled stub size
```

```
struct Configuration {
    int port;
    char ip[16];
};
```

```
int main(){
    Configuration data;
    char filename[256];
    GetModuleFileNameA(NULL, filename, 256);
    ifstream file(filename, ios::binary);
    file.seekg(STUB_SIZE);
    file.read((char*)&data, sizeof(Settings));
    file.close();
    cout << data.ip << endl;
    cout << data.port << endl;
    return 0;
}
```

Builder source code:

```
Code #include <fstream>
#include <iostream>
#include <Windows.h>
```

```
using namespace std;
```

```
#define STUB_NAME "Stub.exe"
```

```
struct Configuration {
    int port;
    char ip[16];
    char built[32];
```

```
};
```

```
int main(){
    Configuration data;
    cout << endl << "Ip: ";
    cin >> data.ip;
    cout << endl << "Port: ";
    cin >> data.port;
    cout << endl << "Built name: ";
    cin >> data.built;
    ifstream file(STUB_NAME, ios::binary);
    ofstream built(data.built, ios::binary);
    built << file.rdbuf();
    file.close();
    built.write((char*)&data, sizeof(Configuration));
    built.close();
    return 0;
}
```

Then we compile the two projects and run the builder and introduce the parameters.

We execute the new .exe generated by the builder and it should show us the parameters that we had injected by the builder.

yuumi - June 5, 2022, 7:18 pm

The more common method on Windows at least legitimately is to use the Resources API. Another would be to allocate a new section in the PE headers, then read and write to that section.

SIM-5195853 - June 6, 2022, 2:04 am

Thanks, I will look at it.

Greetings.

HiddenEye - June 6, 2022, 8:26 am

(Jun 5, 2022 07:18 PM)yuumi Wrote: [\[CITE\]](#) The more common method on Windows at least legitimately is to use the Resources API. Another would be to allocate a new section in the PE headers, then read and write to that section.

that should be the next step for you OP

HFDone - June 6, 2022, 10:54 am

this method called EOF (end of file) there's better methods to use in malware