

Forum:[Hack Forums](#)

Thread: [Anti-VMware \(VMware guest detection \) shellcode version](#)

tty666 - March 9, 2014, 4:00 am

Hello,

I already posted it to ic0de.org but I guess it could be useful here too :)

So looking on the original thread :

<http://www.ic0de.org/showthread.php?9345-SNIPPET-AntiVmWare>

This use magic code on network interface between host & guest VMware to determine if it's a VM or not :)

The original is from Departure (Guy I like you really :)) is already a translation from other author in ASM (MASM32 ? I don't know) to Delphi.

As this stuff is most likely something that AV will not like I had to guess that it should be better to handle this with shellcode which gives opportunity to obfuscate with encryption (Xor ? whatever ...).

Here is my snippet with shellcode :

```
Code Function AntiVMWareShellcode : Boolean;
const
AntiVM : array[0..33] of Byte = (
    $52,$51,$53,$B8,$68,$58,$4D,$56,$BB,$00,$00,$00,$00,$B9,$0A,$00,$00,$00,$BA,$58,
    $56,$00,$00,$ED,$81,$FB,$68,$58,$4D,$56,$5B,$59,$5A,$C3);
begin
    Result := True;
    try
        asm
            LEA EBX,AntiVM[0];
            CALL EBX;
        end;
    except
        Result:= False;
    end;
end;
```

Grrr...Trolls - February 27, 2015, 8:28 am

OMG I havent talked with departure in a long time! Departure, if you there message me! It's kthx/2u/kthxdie we did the hosting shit a while ago that failed lol... Dont worry just want to chat not trying that again O_o lol

Sorry to break it to ya, doesnt work... At least on win7 - errors out "priveleged instruction"