

Forum:[Hack Forums](#)

Thread: [ASM RDTSC VirtualMachine Detector](#)

SIM-1866423 - September 2, 2015, 9:22 am

PHP Code

```
<?php
```

Description

The rdtsc (Read Time-Stamp Counter)

instruction is used to determine how many CPU ticks took place since the processor was reset.

It is commonly used as a timing defense (anti-debugging technique).

PHP Code

```
<?php
```

```
;Concat : b3mb4m@tuta.io
```

```
;nasm -f elf testvm.asm
```

```
;gcc -m32 -o testvm testvm.o
```

```
extern printf
```

```
section .text
```

```
global main
```

```
main:
```

```
mov ebx,0x0A
```

```
loop:
```

```
push ebp ;Set stack frame
```

```
mov ebp,esp
```

```
xor edi,edi
```

```
xor ecx,ecx
```

```
rdtsc
```

```
add edi,eax
```

```
rdtsc
```

```
sub eax,edi
```

```
push eax
```

```
add [total],eax
```

```
push dword printfmat
```

```
call printf
```

```
add esp, 8
```

```
mov esp, ebp
```

```
pop ebp
```

```
dec ebx
```

```
jnz loop
```

```
jz average
```

average:

```
xor eax,eax
xor edx,edx
mov eax,[total]
mov ecx,0x0A
div ecx
```

;Divinded : EDX:EAX

;Quotient : EAX

;Remainder : EDX

```
push eax
push dword printfmat2
call printf
```

```
cmp eax,0xc8
jg vm
jl notvm
```

vm:

```
xor ebx,ebx
push ebx
push vmdetect
call printf
jmp exit
```

notvm:

```
xor ebx,ebx
push ebx
push vmnotpresent
call printf
jmp exit
```

exit:

```
xor eax,eax
inc al
int 0x80
```

section .data

```
vmdetect: db "VM Detected", 10, 0
vmnotpresent db "VM not present", 10, 0
printfmat: db "RDTSC difference : %d", 10, 0 ; The printf format, "\n",'0'
printfmat2: db "RDTSC average : %d ", 10, 0
total: dd 0
```

Results,
PHP Code
<?php

Intel(R) Pentium(R) Dual CPU E2180 @ 2.00GHz

RDTSC difference : 110
RDTSC difference : 110
RDTSC difference : 110
RDTSC difference : 110
RDTSC difference : 100
RDTSC difference : 110
RDTSC difference : 110
RDTSC difference : 100
RDTSC difference : 110
RDTSC difference : 110
RDTSC average : 108
VM not present <---

Assembly, very entertaining ?

h4arck - September 4, 2015, 12:36 am

"jmp exit" in the label "notvm" and "jz average" in the label "loop" are innecesary..

When i go home i test

SIM-1866423 - September 4, 2015, 2:22 am

(Sep 4, 2015 12:36 AM)h4arck Wrote: [\[CITE\]](#) "jmp exit" in the label "notvm" and "jz average" in the label "loop" are innecesary..

When i go home i test

If you are talking about technical issue, explain me why.I would love to learn ..

h4arck - September 4, 2015, 8:32 am

(Sep 4, 2015 02:22 AM)b3mb4m Wrote: [\[CITE\]](#) If you are talking about technical issue, explain me why.I would love to learn ..

Sorry by my english..

Well.. im not a "master" with asm i think that my level with this language is 6/10

When i said that some jumps are innecesary, i want to said that some jumps are innecesary.

Example:

PHP Code

```
<?php  
mov al, 20  
jmp myminijump  
myminijump:  
add al, 20
```

I think that your code works fine.. but you can reduce the size of your code (thats its ironic with asm ?).

I have a question.. when the code take the decision to determinate if is a virtualmachine or not.. is compared with the value '0xc8'.. where you pick this value??

In the same part of your code where you put the jumps 'jg vm, jl notvm' if eax is exactly 0xc8 no

one jump is processed so the program continue to 'vm' label. Maybe you want process in this situation, just only need add the letter 'e' so 'jge or jle'. Both jump have the same size. 1 byte.

Again, sorry by my english. I would love to learn, too. ??

SIM-1866423 - September 4, 2015, 2:43 pm

If problem only unnecessary lines thats fine to me, because its not shellcode hehe :P

0xc8 its just number(200) for compare CPU ticks, commonly if computer is not work on virtualmachine that number around 50-200 but if on virtual machine +1000. That's how we can detect virtual machine with rdtsc instruction(Read Time-Stamp Counter).

You are right about jumps .. its bug, my mistaken. Can be fix with (again unnecessary lines lol);

PHP Code

```
<?php
```

```
je vm
```

```
;or
```

```
je notvm
```

[Also highly recommend this source if u are interest with this topic.](#)

ng-Coder - October 28, 2015, 12:48 pm

I can see HF tag this as PHP code ?