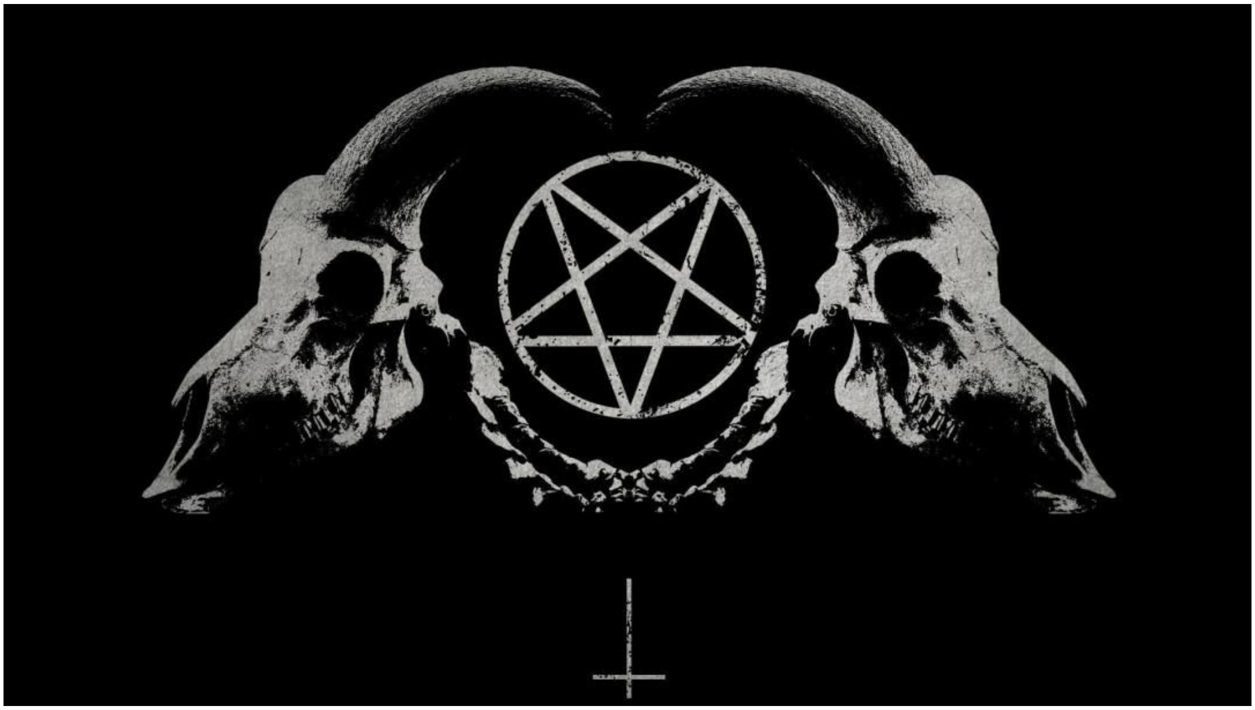
21 Ways To Reset A Register

vx-underground.org archive // z0mbie



One night, from nehu do this text was written. Here are all kinds of ways to reset the registers - from simple to the most sophisticated, but that's what's not there - so it is a complete perversion, such as zeroing one by one bit, auto generated code, etc.

1. Zero MOV

```
mov r, 0
```

2. Replace MOV with equivalent PUSH and POP

```
push
pop r
```

3. The most hacking way: subtract the register from itself.

```
sub r, r
```

4. Xorim (also a good way ... but ... somehow not that ...) Along the way (c) on the name of the painting: "Arvihacker, vorzori vord in mind"

```
xor r, r
```

5. Also a good way, really fuck nobody needed.

```
and r, 0
```

6. More cleverly: multiply by 0.

```
imul r, 0
```

7. Shift (not to be confused with the jump). X1 + X2 in total is greater than / equal to the size of the register in bits, individually less. Less because it is taken modulo.

```
shr / shl / sal r, x1; X1 <= 31, X2 <= 31, X1 + X2> = 32
shr / shl / sal r, x2;
```

8. More distorted shift.

```
clc
rcr / rcl, X1
clc
rcr / rcl, x2
```

9. Not quite an honest way, but ...

```
or reg, -1
inc / not reg
```

10. Reset (E) CX. (although so can be fucked)

```
loop $
```

11. Flush the EDX.

```
shr eax, 1
cdq
```

11. Zero AL. (AH = AL, AL = 0)

```
aam 1
```

12. Reset AH

```
aad 0
```

13. AL again

```
clc
setalc; opcode: 0xD6
```

14. More cleverly: read 0 from the port (for example, port 81h)

```
mov dx,
in al, dx
```

15. AL again

```
stc
setnc al
```

16. And then someone will climb in the dock. 5 times bsf or bsr.

```
bsf r, r
bsf r, r
bsf r, r
bsf r, r
bsf r, r
```

17. Use the zero descriptor from GDT

```
sgdt [esp-6]
mov r, [esp-4]
mov r, [r]
```

18. We consider zero from the FS segment (PE file)

```
mov r, fs: [10h]; constant to taste, would be zero
```

19. Cycle (I repeat: the main thing here is not fucking)

```
inc / dec r; it's a little long
jnz $ -1
```

20. Call some thread function with curved parameters (return NULL in EAX)

```
call getCurrentObject
```

21. Use the coprocessor

```
fldz
fistp dword ptr [esp-4]
mov eax, [esp-4]
```

22, 23, 24, ...

The following options are also proposed to reset the register:
- scan the SEH handler chain to the victorious zero
- scan the chain of file handles to zero (for this, you must first put in the handle of the open file ring zero, and before that go to zero and open this file)
- read zero from a random file (need random number generator)
- sine calculation from Pi * n (multiply with the FMUL command)
- sorting memory and finding zero as the minimum element
- definition of zero as a constant (in the source)
- create a special macro to generate zero
- run the virus and count the number of remaining files

...