Test and Evaluation

Lisa MALIPHOL

Table 1: Anomalous Sources

ip.src
192.168.12.34

Table 2: Anomalous Destinations

ip.dst
192.168.12.34

Table 3: Anomalous Source / Modbus Unit Pairs

IP_DST_MODBUS_UNIT_ID	ip.dst	mbtcp.modbus.unit_id
192.168.12.253/	192.168.12.253	
192.168.12.253/0	192.168.12.253	0
192.168.12.34/	192.168.12.34	
192.168.12.34/0	192.168.12.34	0

Table 4: Anomalous Source / MAC Address Pairs

IP_SRC_MAC_ADDR	ip.src	eth.src
192.168.12.34/08:00:27:4a:25:6c	192.168.12.34	08:00:27:4a:25:6c

Table 5: Anomalous Source / MODBUS Function Code Pairs

IP_SRC_MOD_FUNC	ip.src	mbtcp.modbus.func_code
192.168.12.253/	192.168.12.253	
192.168.12.253/90	192.168.12.253	90
192.168.12.34/	192.168.12.34	
192.168.12.34/90	192.168.12.34	90
192.168.12.53/	192.168.12.53	

Table 6: Differences in Frequency of Source/Function Code

ip.src	ip.dst	mbtcp.modbus.func_code
192.168.12.253	192.168.12.53	4
192.168.12.53	192.168.12.253	4

Table 7: (cont.)

avgFrequencySec.n	avgFrequencySec.a	avgFrequencySec.diff
33.14408	33.08108	0.0630013
33.14408	33.08108	0.0630013

Table 8: Differences in Frequency of Source/Function Code/Reference Number

ip.src	ip.dst	mbtcp.modbus.func_code	mbtcp.modbus.reference_num
192.168.12.53	192.168.12.253	4	0
192.168.12.53	192.168.12.253	4	1
192.168.12.53	192.168.12.253	4	2
192.168.12.53	192.168.12.253	4	3

Table 9: cont.

avgFrequncySec.n	avgFrequncySec.a	avgFrequencySec.diff
13.675258	13.714286	-0.0390280
15.618557	15.567568	0.0509891
1.962069	1.959184	0.0028853
1.962004	1.959184	0.0028198

avgFrequncySec.n	avgFrequncySec.a	avgFrequencySec.diff

```
       frame.number frame.time_relative frame.time_delta frame.len
    1:            3            0.185127         0.004811        65
    2:            5            0.196988         0.011572        65
    3:            7            0.208054         0.010812        65
    4:            9            0.221087         0.012746        65
    5:           11            0.233086         0.011740        65
   ---
24941:        51349          778.068159         0.010721        65
24942:        51351          778.080318         0.011812        65
24943:        51353          778.093005         0.012338        65
24944:        51355          778.105172         0.011818        65
24945:        51357          778.117466         0.011945        65
       ip.proto ip.version         ip.src           eth.src         ip.dst
    1:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
    2:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
    3:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
    4:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
    5:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
   ---
24941:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
24942:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
24943:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
24944:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
24945:        6          4 192.168.12.252 00:0f:69:0d:55:cd 192.168.12.117
                  eth.dst mbtcp.modbus.unit_id tcp.srcport tcp.dstport
    1: 08:00:27:f9:b1:f1                    1         502        1043
    2: 08:00:27:f9:b1:f1                    1         502        1043
    3: 08:00:27:f9:b1:f1                    1         502        1043
    4: 08:00:27:f9:b1:f1                    1         502        1043
    5: 08:00:27:f9:b1:f1                    1         502        1043
   ---
24941: 08:00:27:f9:b1:f1                    1         502        1043
24942: 08:00:27:f9:b1:f1                    1         502        1043
24943: 08:00:27:f9:b1:f1                    1         502        1043
24944: 08:00:27:f9:b1:f1                    1         502        1043
24945: 08:00:27:f9:b1:f1                    1         502        1043
       mbtcp.prot_id mbtcp.trans_id mbtcp.len mbtcp.modbus.func_code
    1:             0            90         5                     4
    2:             0            91         5                     4
    3:             0            92         5                     4
    4:             0            93         5                     4
```

```
    5:             0             94         5                     4
   ---
24941:             0            198         5                     4
24942:             0            199         5                     4
24943:             0            200         5                     4
24944:             0            201         5                     4
24945:             0            202         5                     4
       mbtcp.modbus.reference_num mbtcp.modbus.word_cnt mbtcp.modbus.data
    1:                                              NA              12:e7
    2:                                              NA              00:70
    3:                                              NA              00:70
    4:                                              NA              00:70
    5:                                              NA              00:70
   ---
24941:                                              NA              00:70
24942:                                              NA              00:70
24943:                                              NA              00:70
24944:                                              NA              00:70
24945:                                              NA              00:50
```

Table 10: Requests Summary

frame.number	frame.time_relative	frame.time_delta	frame.len	ip.proto	ip.version
Min. : 3	Min. : 0.1851	Min. :0.001642	Min. :65	6:24945	4:24945
1st Qu.:12840	1st Qu.:198.0572	1st Qu.:0.011584	1st Qu.:65	NA	NA
Median :25679	Median :388.5154	Median :0.011861	Median :65	NA	NA
Mean :25679	Mean :388.8184	Mean :0.011772	Mean :65	NA	NA
3rd Qu.:38518	3rd Qu.:584.1774	3rd Qu.:0.012571	3rd Qu.:65	NA	NA
Max. :51357	Max. :778.1175	Max. :0.775146	Max. :65	NA	NA

ip.src	eth.src	ip.dst	eth.dst
192.168.12.117: 0	00:0f:69:0d:55:cd:24945	192.168.12.117:24945	00:0f:69:0d:55:cd: 0
192.168.12.252:24945	08:00:27:f9:b1:f1: 0	192.168.12.252: 0	08:00:27:f9:b1:f1:24945

mbtcp.modbus.unit_id	tcp.srcport	tcp.dstport	mbtcp.prot_id	mbtcp.trans_id	mbtcp.len
: 0	1043: 0	1043:24945	: 0	Min. : 0.0	Min. :5
1:24945	502 :24945	502 : 0	0:24945	1st Qu.: 64.0	1st Qu.:5
NA	NA	NA	NA	Median :128.0	Median :5
NA	NA	NA	NA	Mean :127.6	Mean :5
NA	NA	NA	NA	3rd Qu.:191.0	3rd Qu.:5
NA	NA	NA	NA	Max. :255.0	Max. :5

mbtcp.modbus.unit_id	tcp.srcport	tcp.dstport	mbtcp.prot_id	mbtcp.trans_id	mbtcp.len

mbtcp.modbus.func_code	mbtcp.modbus.reference_num	mbtcp.modbus.word_cnt
: 0	:24945	Min. : NA
4:24945	0: 0	1st Qu.: NA
NA	1: 0	Median : NA
NA	2: 0	Mean :NaN
NA	3: 0	3rd Qu.: NA
NA	NA	Max. : NA
NA	NA	NA's :24945