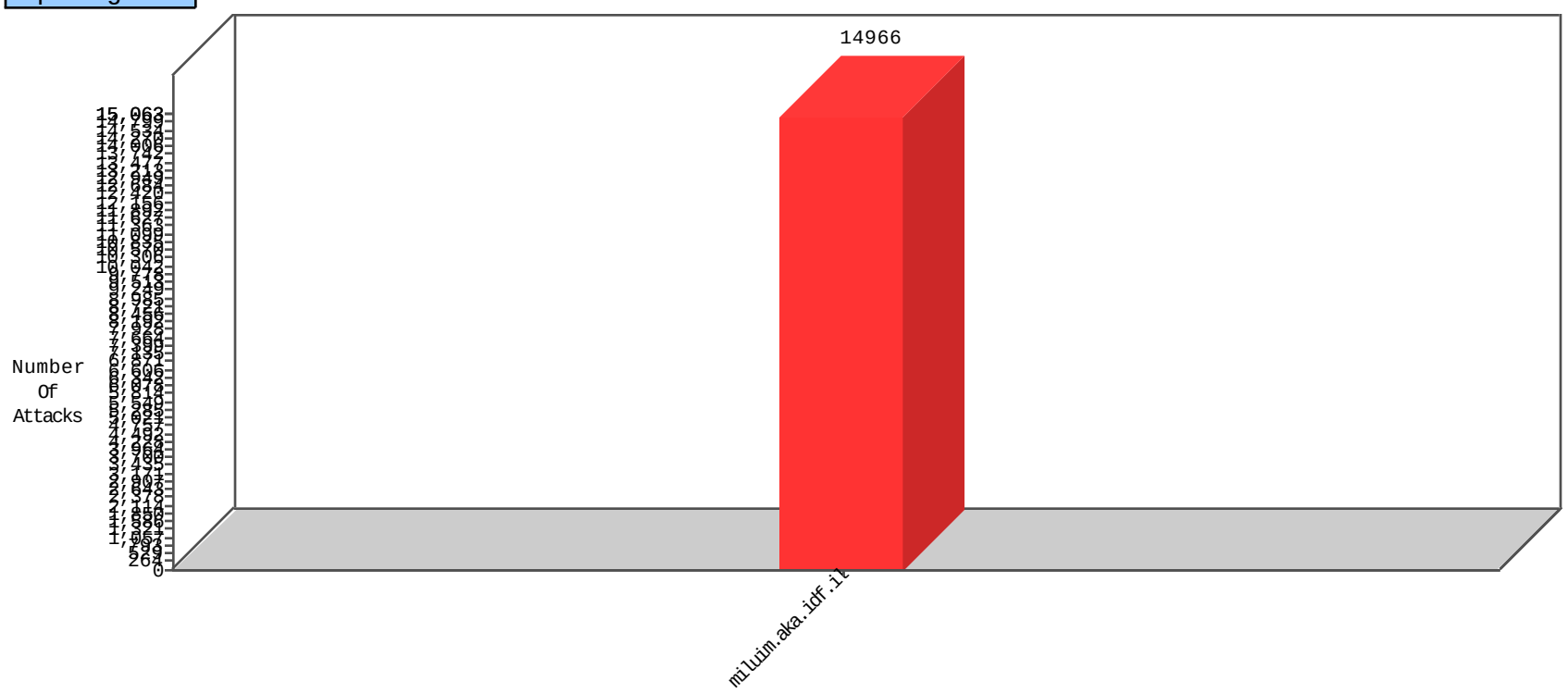
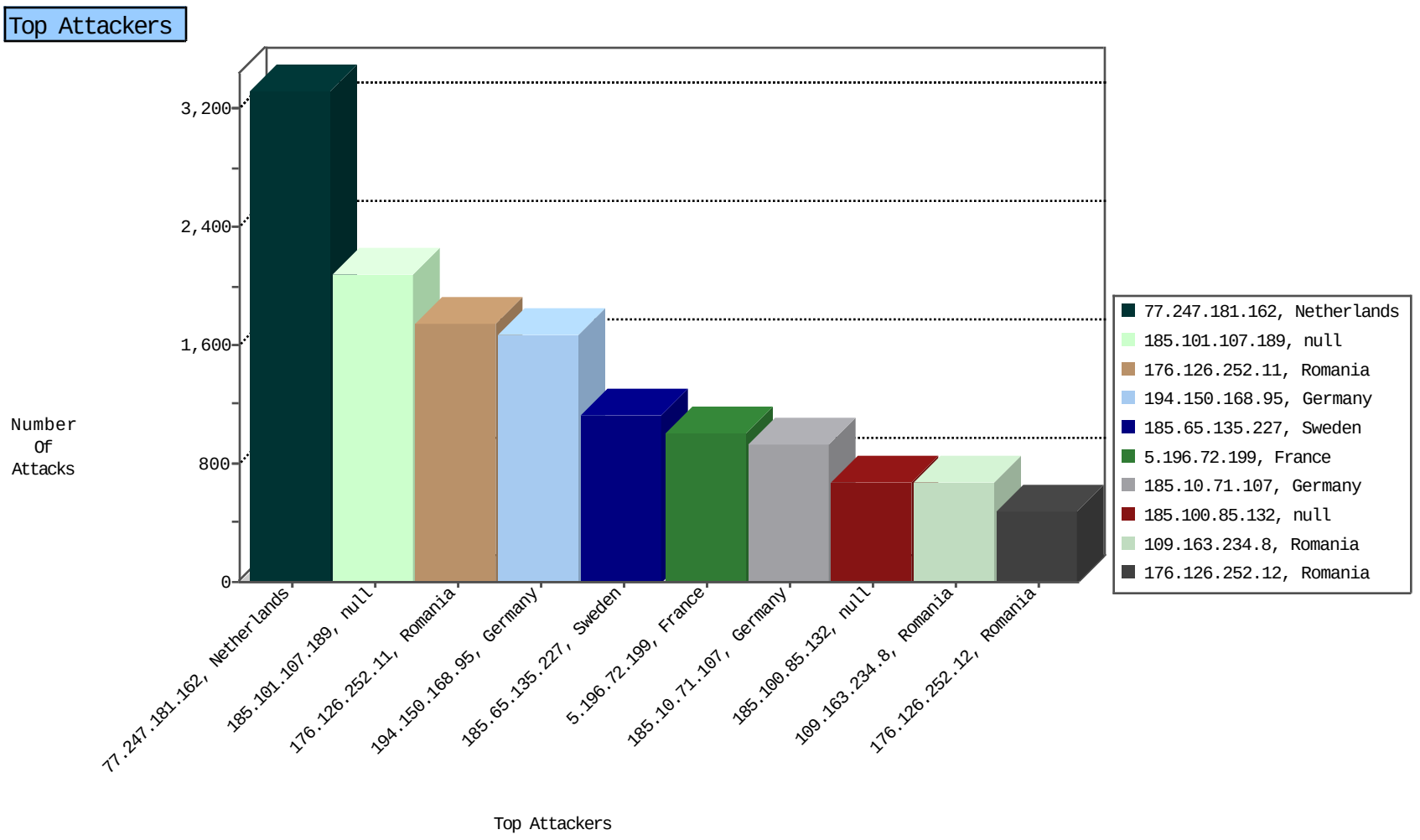
01-08-2016 to 01-09-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-08-2016 to 01-09-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
85.250.89.211	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	DP-Tehila	3
115.239.228.10	China	147.237.0.120	miluim.aka.idf.il	Frk_Under_Attack_Con_Http	drop	BBL-Frankfurt	2
115.239.228.10	China	147.237.0.120	miluim.aka.idf.il	Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	1

01-08-2016 to 01-09-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-08-2016 to 01-09-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
176.50.139.113	Russian Federation	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
109.111.182.98	Russian Federation	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.15	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
158.255.2.52	Russian Federation	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	United Kingdom	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.201.227.7	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	Canada	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
131.109.15.15	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -f -sS	1
131.109.15.15	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
168.63.206.180	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-08-2016 to 01-09-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	121828
185.100.85.132		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	104445
66.249.81.230	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	33043
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	26293
185.29.8.132	Sweden	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22113
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	5714
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	5287
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2420
185.3.146.229	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
149.88.40.63	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1452
80.178.98.173	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1305
108.61.123.69	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1190
108.61.123.67	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1146
144.24.20.233	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1036
68.180.229.121	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	995
108.61.122.139	France	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	943
212.16.104.33	Finland	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	790
83.149.124.214	Netherlands	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	655
149.78.97.64	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	512
149.88.232.225	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	502
149.78.229.180	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	453
149.78.241.99	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	432
149.78.134.165	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	308
79.178.21.203	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
79.177.202.241	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	217
66.249.75.219	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	213
149.78.20.188	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	192
176.10.99.203	Switzerland	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	190
149.78.255.165	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	182
31.168.172.144	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
79.177.202.241	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	169
109.65.35.176	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.181.199.21	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.201.143.40	Germany	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	140
149.88.160.38	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	134
149.88.27.88	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	133
66.249.75.235	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	132
130.193.51.91	Russian Federation	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	128
37.130.227.133	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	127
149.78.224.150	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	125
194.150.168.95	Germany	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	118
90.213.33.139	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	110
149.78.245.130	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	109
149.78.60.229	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.200.227	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.228.221	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	105
142.4.213.25	Canada	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	104
66.102.9.90	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	101
62.219.198.6	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
51.175.93.165	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	100

01-08-2016 to 01-09-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.101.107.189		147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2081
77.247.181.162	Netherlands	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1793
176.126.252.11	Romania	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1749
194.150.168.95	Germany	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1605
77.247.181.162	Netherlands	147.237.0.120	miluim.aka.idf.i	Too Many of the Same Response Code (404) in IP from 77.247.181.162	Block	1536
185.65.135.227	Sweden	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1136
5.196.72.199	France	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1014
185.10.71.107	Germany	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	939
185.100.85.132		147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	681
109.163.234.8	Romania	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	674
176.126.252.12	Romania	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	474
109.163.234.5	Romania	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	449
198.50.200.135	Canada	147.237.0.120	miluim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	392
198.50.145.72	Canada	147.237.0.120	miluim.aka.idf.i	Too Many of the Same Response Code (404) in IP from 198.50.145.72	Block	316
194.150.168.95	Germany	147.237.0.120	miluim.aka.idf.i	Too Many of the Same Response Code (404) in IP from 194.150.168.95	Block	76
46.116.94.41	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 46.116.94.41	Block	14
79.183.28.182	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 79.183.28.182	Block	7
2.54.156.138	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 2.54.156.138	Block	6
77.247.181.162	Netherlands	147.237.0.120	miluim.aka.idf.i	Too Many 404: Response Code per IP	Block	2
194.150.168.95	Germany	147.237.0.120	miluim.aka.idf.i	Too Many 404: Response Code per IP	Block	1
85.64.2.76	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/resource/userfollowresource/create/	Block	1
46.19.86.108	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1408-he/miluim.aspxâ€?â€Ž	Block	1
217.132.117.205	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/1316-he/miluim/aspx	Block	1
198.50.145.72	Canada	147.237.0.120	miluim.aka.idf.i	Too Many 404: Response Code per IP	Block	1
46.116.94.41	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1316-he/miluim.asp	Block	1

01-08-2016 to 01-09-2016