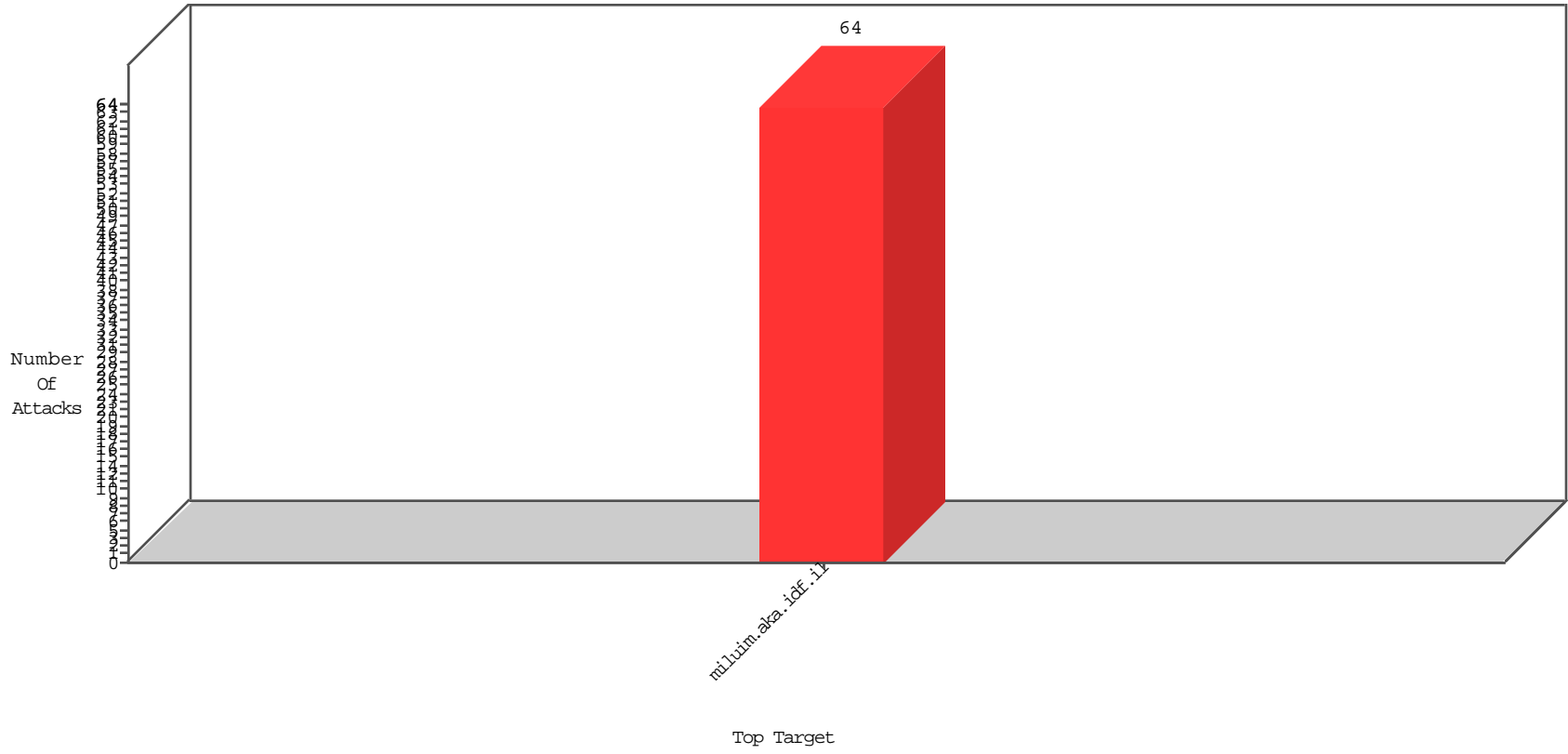


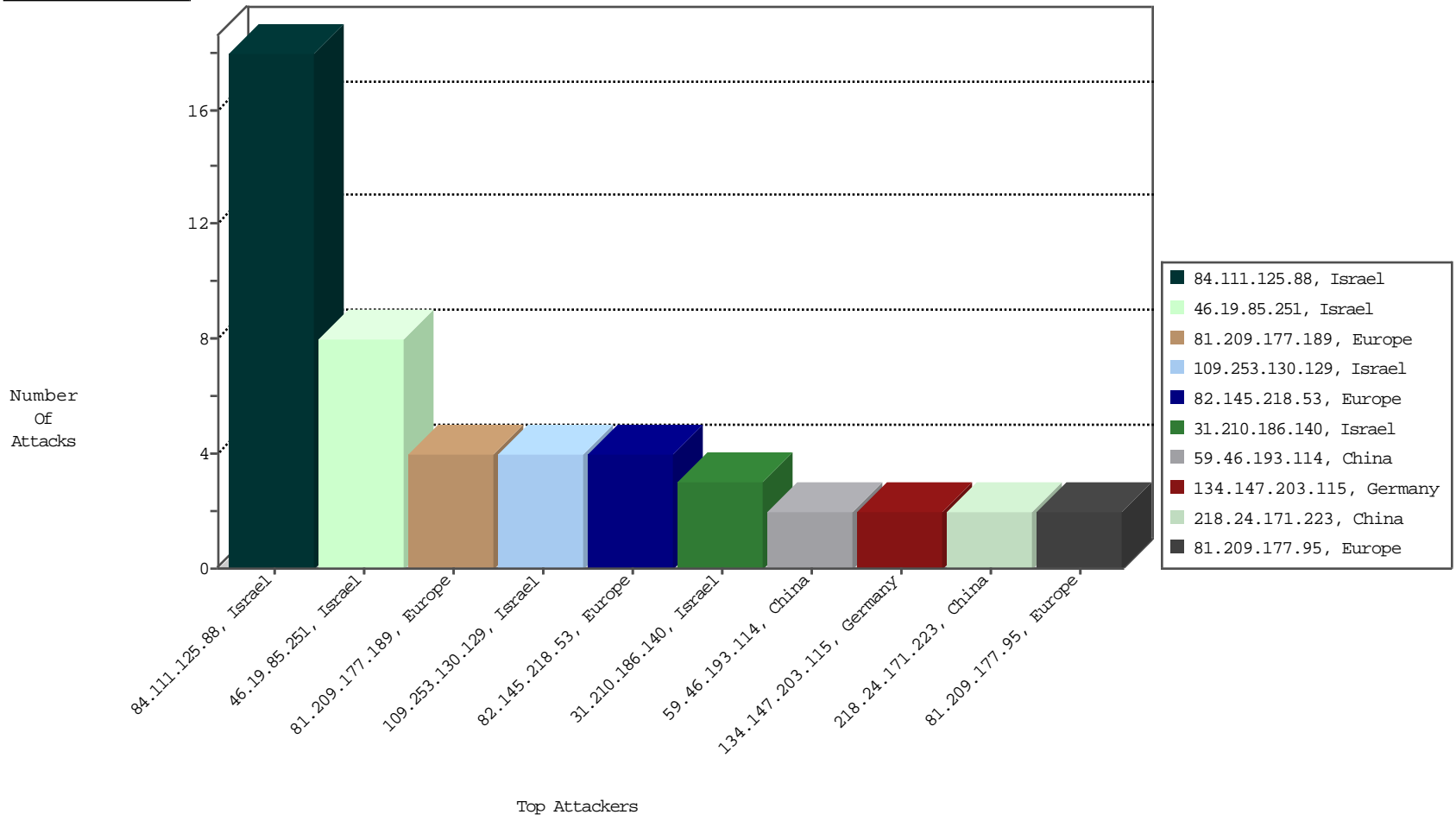
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
84.111.125.88	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	EEL-Isreal	18
82.145.218.53	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	4
134.147.203.115	Germany	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	2
183.2.172.4	China	147.237.0.120	miluim.aka.idf.il	L4 Source or Dest Port Zero	drop	DP-Tehila	2
184.105.139.110	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
185.40.4.98		147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
205.209.185.11	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
71.6.167.142	United States	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1

02-27-2016 to 02-28-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
59.46.193.114	China	147.237.0.120	miluim.aka.idf.il	GPL SCAN nmap TCP	2
109.253.130.129	Israel	147.237.0.120	miluim.aka.idf.il	GPL SCAN myscan	2
218.24.171.223	China	147.237.0.120	miluim.aka.idf.il	GPL SCAN nmap TCP	2
66.249.64.1	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	2
109.253.130.129	Israel	147.237.0.120	miluim.aka.idf.il	INDICATOR-SCAN myscan	2
120.194.193.15	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.18.17.201	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
146.185.250.2	Russian Federation	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.173		147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	China	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
79.181.137.69	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
109.66.38.31	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	954
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	864
109.64.29.27	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
109.65.152.207	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
109.67.166.179	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
2.52.186.167	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
36.253.255.56	Nepal	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	149
77.127.2.70	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.65.55.230	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
46.19.86.245	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.186.81	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.125.23		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.180.162	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
5.28.171.204	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.176.4.212	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
37.26.149.143	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
37.142.185.39	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	87
37.142.185.39	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	81
79.178.31.102	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
79.180.39.73	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
37.142.136.98	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	45
198.204.249.34	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
37.142.136.98	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
2.54.132.146	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.180.13.159	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.60.110	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	34
46.19.85.185	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	32
36.253.255.56	Nepal	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
46.19.85.98	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.142	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
5.29.213.215	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
94.230.147.162	Czech Republic	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
109.67.6.47	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.106	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.142	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
79.180.204.39	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.61.10	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.196.249	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.148.124	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.121.105.72	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
85.65.190.187	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
149.78.85.174	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.183.197.83	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.210.187.195	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
84.109.202.158	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.154	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.201.30	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.120.239.184	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9

02-27-2016 to 02-28-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.209.177.189	Europe	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 81.209.177.189	Block	3
31.210.186.140	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version	Block	1
81.209.177.95	Europe	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 81.209.177.95	Block	1
46.19.85.251	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version	Block	1
198.204.249.34	United States	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/./shared/usercontrols/footer/1230-he/miluim.aspx	Block	1
46.19.85.251	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Malformed URL from 46.19.85.251	Block	1
31.210.186.140	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL www.miluim.aka.idf.il	Block	1
81.209.177.95	Europe	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.behatsdaa.org.il	Block	1
46.19.85.251	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL _pk_ses.104.b624=*	Block	1
198.204.249.34	United States	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/./shared/usercontrols/headerupper/	Block	1
46.19.85.251	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unknown HTTP Request Method from 46.19.85.251	Block	1
31.210.186.140	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method Host: in URL www.miluim.aka.idf.il	Block	1
46.19.85.251	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Abnormally Long Request from 46.19.85.251	Block	1
46.19.85.251	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method 24=6764959e967be636.1456583417.1.1456583417.1456583417.; in URL _pk_ses.104.b624=*	Block	1
46.19.85.251	Israel	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
81.209.177.189	Europe	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.251	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Illegal HTTP Version from 46.19.85.251	Block	1

02-27-2016 to 02-28-2016