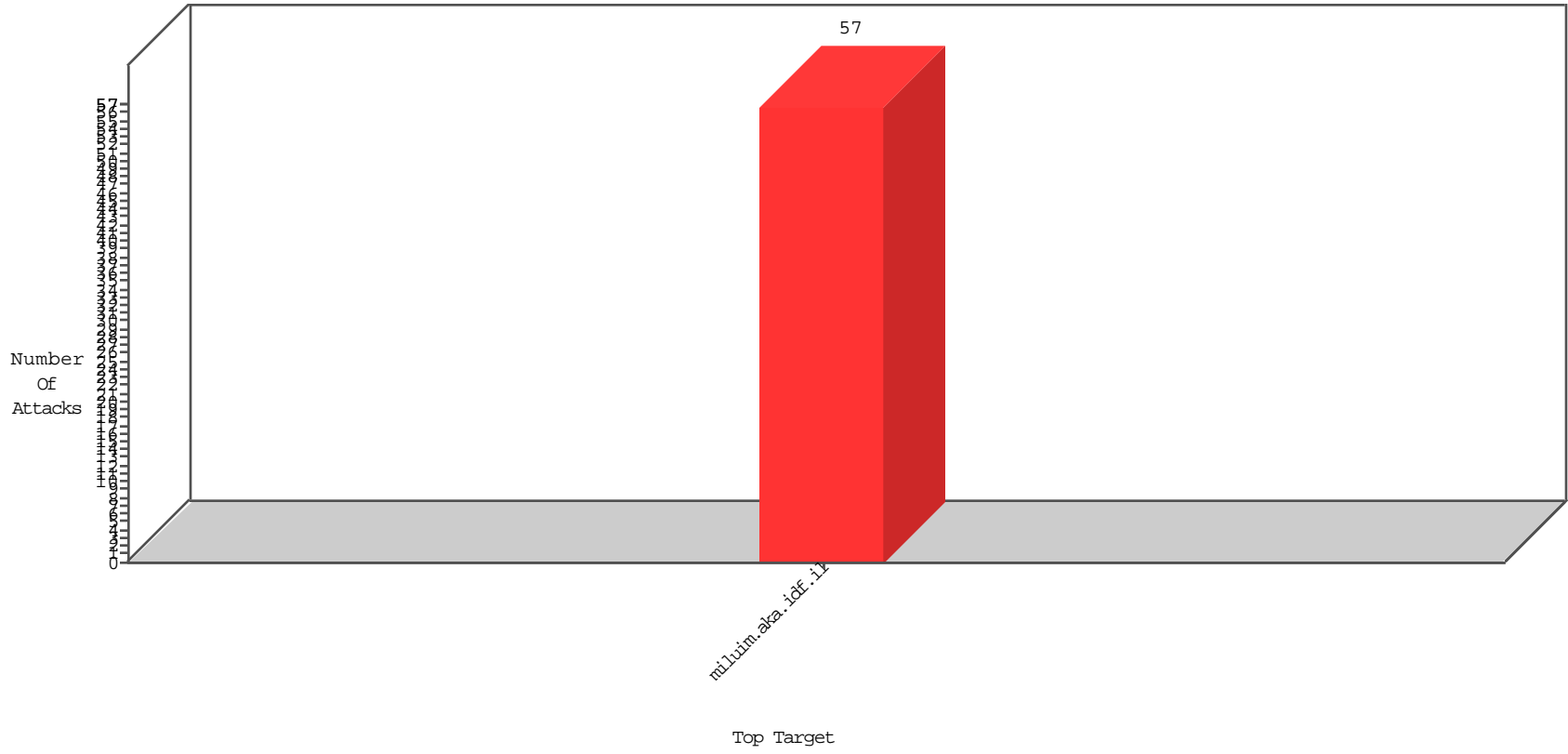


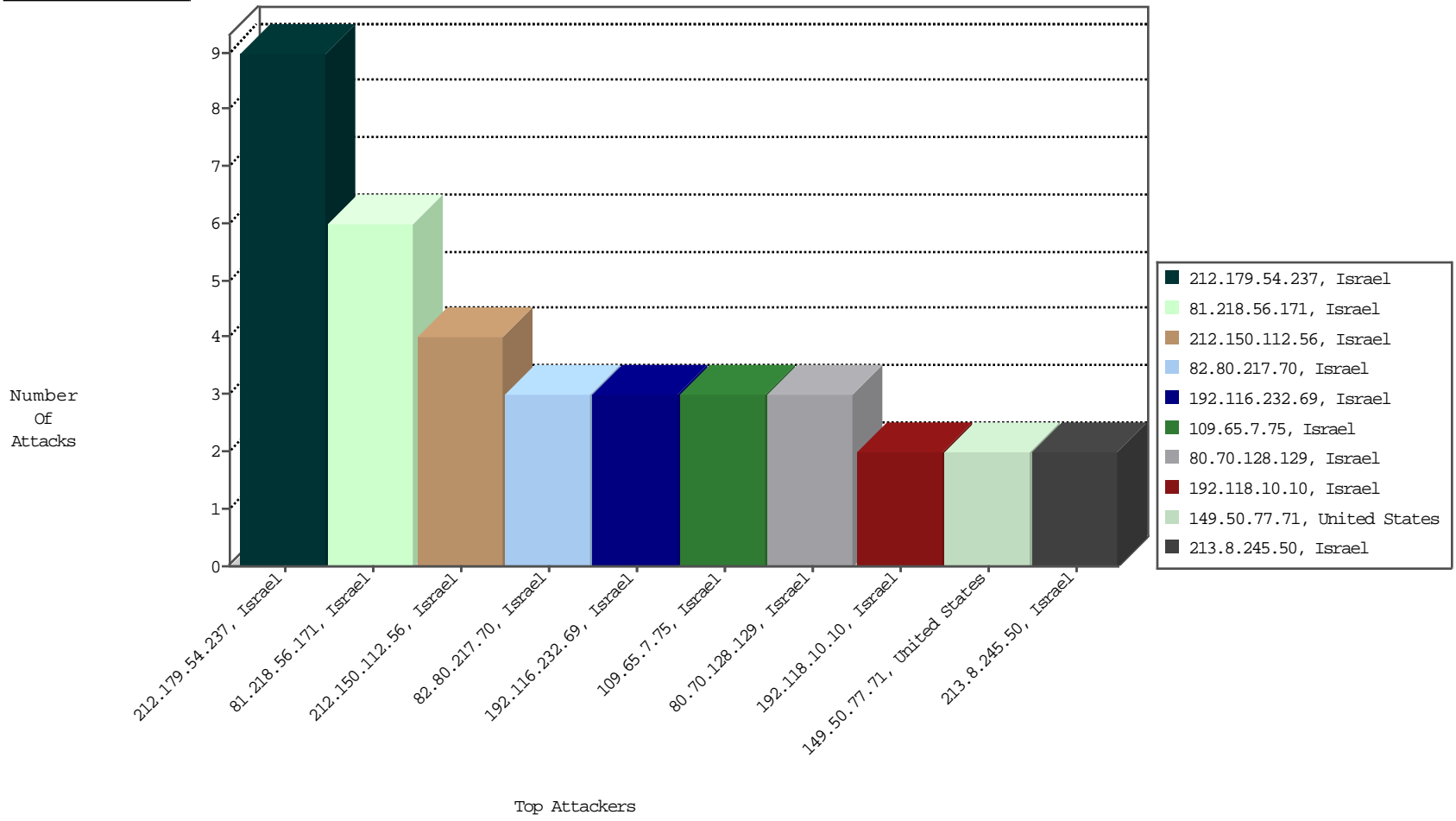
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.54.237	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	9
80.70.128.129	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	3
82.80.217.70	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	3
109.65.7.75	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	3

01-31-2016 to 02-01-2016

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
60.217.72.16	China	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	Lithuania	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
222.170.70.222	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
2.52.156.81	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.180.126.182	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.54.177.27	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1521
79.176.3.117	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1444
62.219.238.10	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	468
84.228.192.177	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
84.228.202.188	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.181.118.105	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.178.176.179	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
2.54.40.220	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
109.66.192.43	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	279
46.19.86.92	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
79.180.216.110	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
2.52.33.201	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
2.54.182.84	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
2.54.187.75	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
87.68.23.97	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.126.62		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.32.232	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.179.213.233	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	140
2.52.31.93	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
209.88.157.156	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	81
80.178.201.148	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	36
46.19.85.55	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.55	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
209.88.157.156	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	34
188.120.148.202	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	31
46.121.105.122	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	29
80.178.138.115	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	27
31.210.188.22	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	27
46.19.85.220	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.86.173	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
31.210.186.239	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
77.126.24.147	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
213.57.163.11	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.86.54	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
213.57.163.11	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
212.235.72.236	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
37.26.148.188	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
199.203.226.21	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.178	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
192.118.117.100	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
212.235.72.236	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
46.19.86.2	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
77.126.24.147	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.85.24	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
192.118.27.253	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	14
85.130.175.9	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
41.230.14.223	Tunisia	147.237.0.120	miluim.aka.idf.i	drop	SAM rule	drop	13
192.118.27.253	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.218.56.171	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	4
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/scriptresource.axd parameter wb48617274	Block	2
192.118.10.10	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	2
212.150.112.56	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	2
149.50.77.71	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/login	Block	2
81.218.56.171	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/1935.gif	Block	2
95.86.124.93	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 95.86.124.93	Block	1
37.142.64.36	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
213.151.59.82	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjkidy7ottkahvclw8khvw-boeqfggimaa&usg=afqjcne5p7m9pmcma58u2cjzfnfg7azoamw	Block	1
194.72.238.241	United Kingdom	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/xyzyzy	Block	1
158.116.225.93	United States	147.237.0.120	miluim.aka.idf.i	Suspicious Response Code	Block	1
213.8.245.50	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/1935.gif	Block	1
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/1935.gif	Block	1
95.86.124.93	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewipy5sjlttkahwj73ikhrx2djgqfggimaa&usg=afqjcne5p7m9pmcma58u2cjzfnfg7azoamw	Block	1
37.142.64.36	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
212.150.112.56	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.150.112.56	Block	1
182.118.53.217	China	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
81.218.241.26	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/	Block	1
31.154.168.26	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/https://mysearch.avg.com/	Block	1
213.8.245.50	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
141.212.122.81	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /x	Block	1
61.135.190.200	China	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
185.89.217.233		147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/./images/shared/hp/hp_icon.png	Block	1
95.86.104.120	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewih6eav_ntkahuffswkhzwib0oqfggimaa&usg=afqjcne5p7m9pmcma58u2cjzfnfg7azoamw	Block	1
37.60.42.11	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewiokrjyynpkahxivrqkhu2-ccoqfggimaa&usg=afqjcne5p7m9pmcma58u2cjzfnfg7azoamw	Block	1
213.8.245.58	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/scriptresource.axd parameter wb48617274	Block	1
194.72.238.241	United Kingdom	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 194.72.238.241	Block	1
212.150.112.56	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1