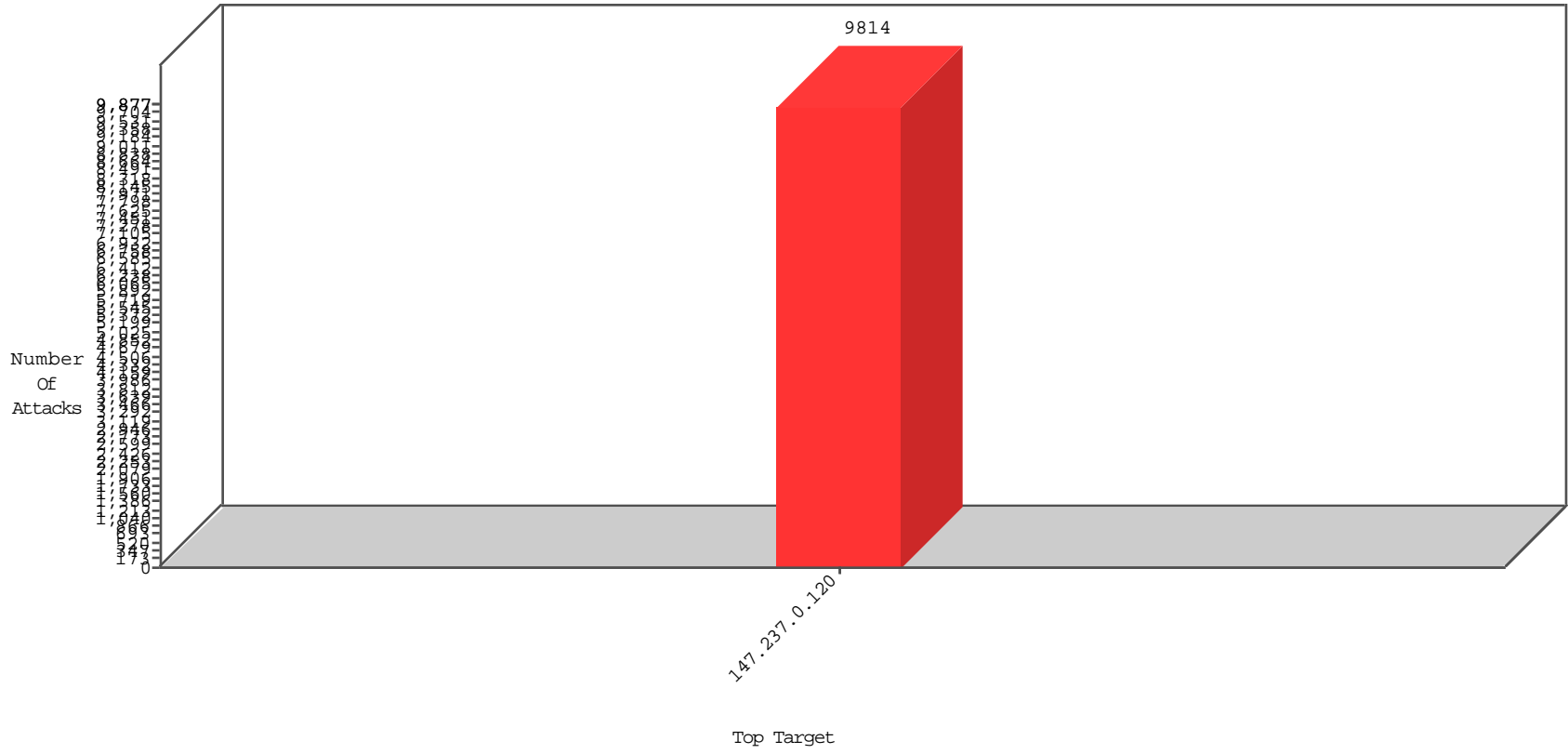


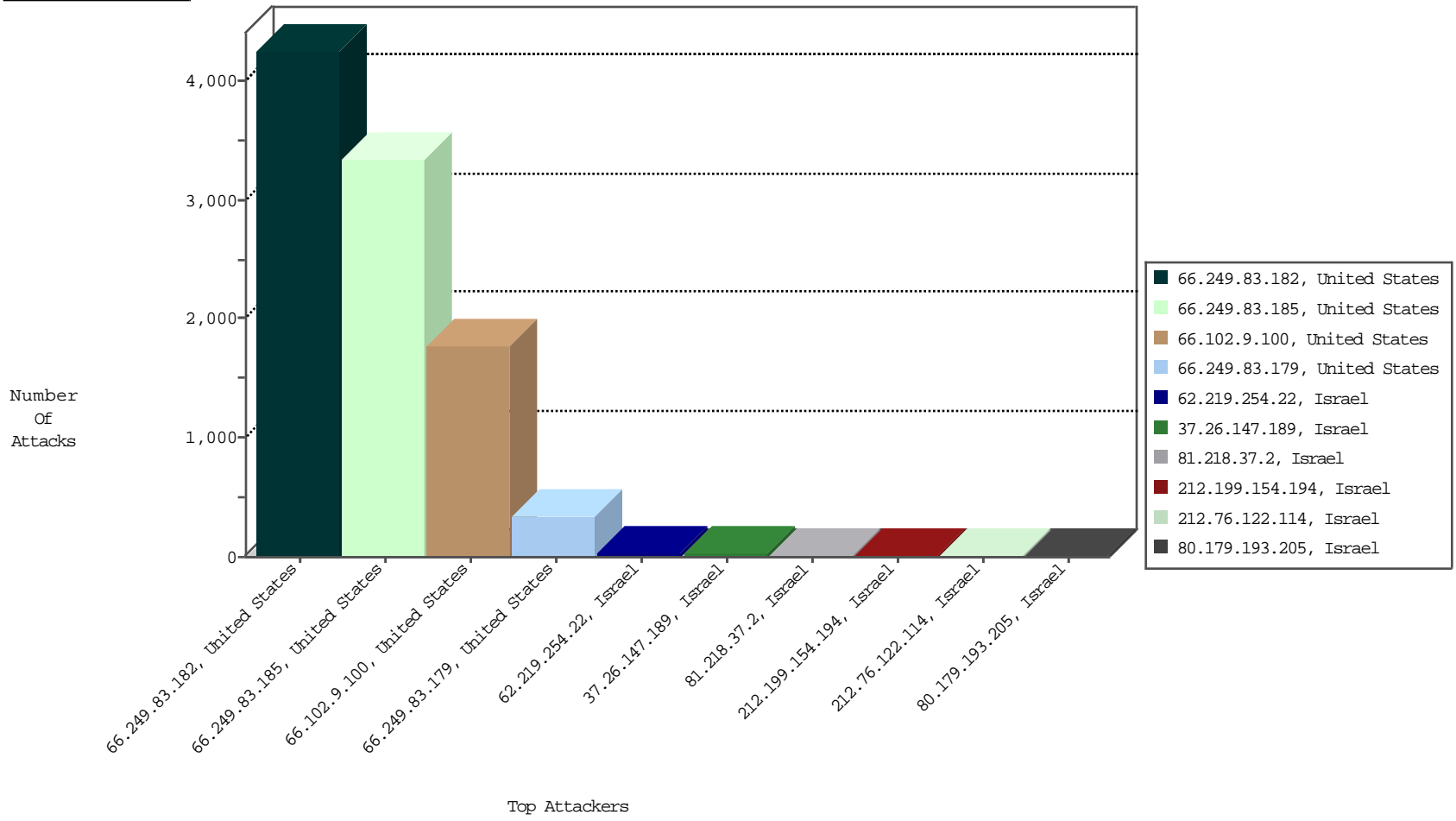
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.83.182	United States	147.237.0.120		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	4266
66.249.83.185	United States	147.237.0.120		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	3352
66.102.9.100	United States	147.237.0.120		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1783
66.249.83.179	United States	147.237.0.120		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	331
62.219.254.22	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	27
37.26.147.189	Israel	147.237.0.120		Invalid TCP Flags	drop	BBL-Israel	6
81.218.56.125	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	1
37.26.146.157	Israel	147.237.0.120		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1

11-03-2015 to 11-04-2015

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
37.26.147.189	Israel	147.237.0.120		POLICY-OTHER TCP packet with urgent flag attempt	15
188.138.9.51	Germany	147.237.0.120		ET SCAN NMAP -sS window 1024	1
2.226.65.19	Italy	147.237.0.120		ET SCAN Potential SSH Scan	1
115.72.103.148	Vietnam	147.237.0.120		ET SCAN Potential SSH Scan	1
173.14.213.230	United States	147.237.0.120		ET SCAN NMAP -sS window 4096	1
173.1.121.85	United States	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
66.249.83.182	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	472235
66.249.83.179	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	465108
66.249.83.185	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	444190
66.249.83.188	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	16027
66.249.83.191	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	13022
66.102.9.80	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	13008
66.102.9.90	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	12779
66.102.9.100	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	9953
109.66.116.240	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2501
2.52.58.14	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
77.125.132.149	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
199.203.62.54	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
149.88.31.11	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	1181
157.55.39.33	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	834
139.181.48.2	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	512
149.78.27.94	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	432
110.32.148.119	Australia	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	384
149.78.50.57	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	376
207.46.13.13	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	352
66.249.75.235	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	333
74.64.121.120	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	323
66.249.83.182	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	304
168.63.200.167	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	299
157.55.39.29	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	293
87.68.48.151	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
125.19.102.130	India	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	282
66.249.75.227	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	279
66.249.83.185	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	273
66.249.75.219	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	255
82.196.42.196	United Kingdom	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	248
66.249.83.179	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	220
167.220.196.186	United Kingdom	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	172
149.78.229.181	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	171
149.88.168.236	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	170
68.180.229.121	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	168
157.55.39.186	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	150
149.78.228.172	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	148
149.88.161.60	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	144
5.28.170.52	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.250.190	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	141
66.249.75.235	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	129
66.249.75.227	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	129
194.9.253.238	United Kingdom	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	128
79.161.20.58	Norway	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	114
66.249.75.219	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	109
207.46.13.150	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	105
149.88.84.111	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	99
157.55.39.185	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	98
149.78.111.208	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	95
149.78.235.81	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	94

11-03-2015 to 11-04-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.218.37.2	Israel	147.237.0.120		Multiple Unauthorized URL Access from 81.218.37.2	Block	5
212.199.154.194	Israel	147.237.0.120		Multiple Unauthorized URL Access from 212.199.154.194	Block	4
212.76.122.114	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	3
168.235.198.224	United States	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/*²³õ´	Block	1
80.179.193.205	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	1
212.199.154.194	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
93.173.39.232	Israel	147.237.0.120		Multiple Unauthorized URL Access from 93.173.39.232	Block	1
77.127.60.124	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	1
192.115.130.253	Israel	147.237.0.120		Unauthorized URL Access to miluim.aka.idf.il/1355/he/miluim.aspx	Block	1
81.218.37.2	Israel	147.237.0.120		Distributed Unknown Parameter on www.miluim.aka.idf.il/scriptresource.axd parameter wb48617274	Block	1
2.52.184.178	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
93.173.39.232	Israel	147.237.0.120		PHP Attempt	Block	1
80.179.193.205	Israel	147.237.0.120		Multiple Unauthorized URL Access from 80.179.193.205	Block	1
77.127.60.124	Israel	147.237.0.120		Distributed PHP Attempt	Block	1
93.173.39.232	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	1
80.179.193.205	Israel	147.237.0.120		PHP Attempt	Block	1
81.218.37.2	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/3/1473.png	Block	1
77.127.60.124	Israel	147.237.0.120		Multiple Unauthorized URL Access from 77.127.60.124	Block	1

11-03-2015 to 11-04-2015