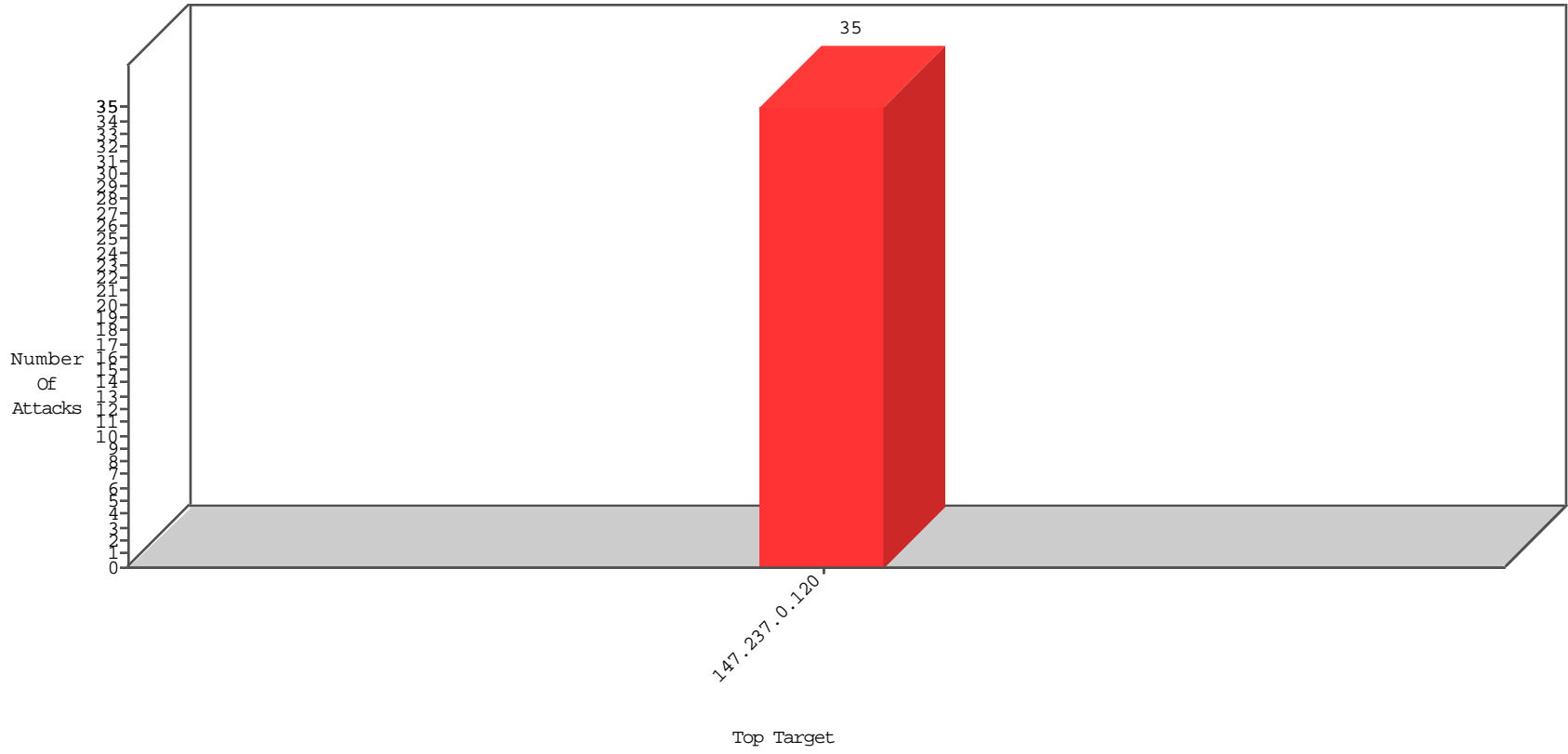


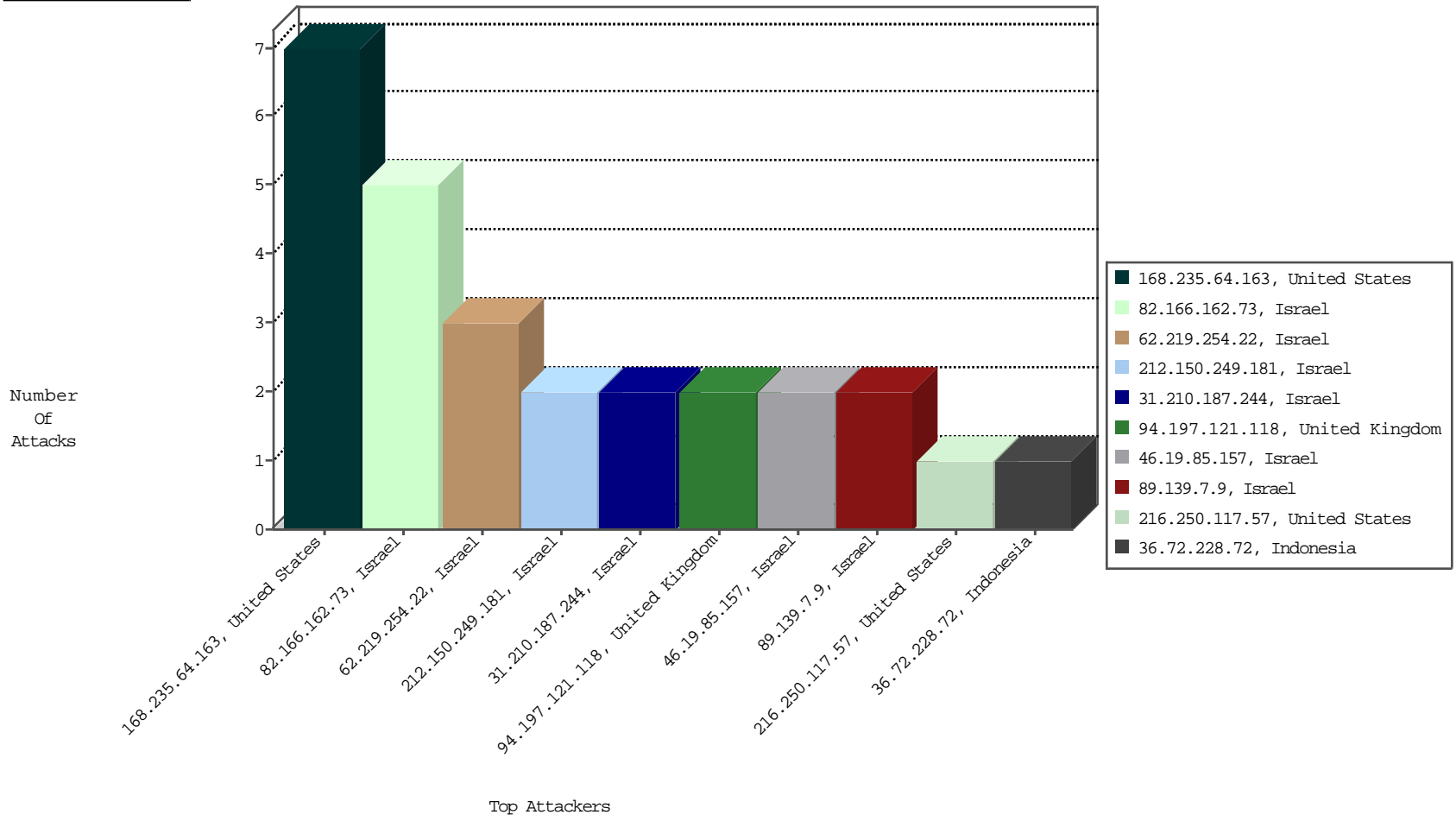
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



11-22-2015 to 11-23-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
62.219.254.22	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	3
94.197.121.118	United Kingdom	147.237.0.120		Invalid TCP Flags	drop	BBL-Frankfurt	2

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.150.249.181	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	2
31.210.187.244	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	2
89.139.7.9	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	2
82.166.162.73	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
168.235.64.163	United States	147.237.0.120		Tehila - Perl LWP with fake user agent	2
31.11.84.158	Macedonia, the Former Yugoslav Republic of	147.237.0.120		ET SCAN NMAP -sS window 1024	1
42.159.26.35	China	147.237.0.120		ET SCAN Potential SSH Scan	1
162.222.185.165	United States	147.237.0.120		ET SCAN Potential SSH Scan	1
216.250.117.57	United States	147.237.0.120		ET SCAN Potential SSH Scan	1
36.72.228.72	Indonesia	147.237.0.120		ET SCAN NMAP -sS window 4096	1
132.70.66.12	Israel	147.237.0.120		ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
222.21.43.56	China	147.237.0.120		ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
137.135.176.145	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	12229
84.95.1.178	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
84.228.9.42	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.54.10.50	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
82.81.14.45	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.176.105.51	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2034
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1738
66.249.93.207	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1603
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1506
192.232.81.1	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1150
149.78.38.162	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1078
199.201.66.0	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	744
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	581
64.79.85.205	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	536
66.249.81.230	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	509
66.249.79.112	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	434
66.249.79.114	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	433
149.78.38.149	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	406
66.249.79.110	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	397
149.78.29.167	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	381
157.55.39.229	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	361
94.197.121.118	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	360
40.77.167.104	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	309
149.88.6.220	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	289
40.77.167.50	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	259
134.191.238.106	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	241
40.77.167.43	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	239
157.55.39.3	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	236
149.78.237.176	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	230
2.54.45.213	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
149.78.147.185	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	213
40.77.167.10	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	192
157.55.39.142	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	190
66.249.79.112	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	183
149.78.255.61	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	180
149.88.30.196	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	177
149.88.7.101	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	176
66.249.79.114	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	165
24.12.74.89	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	164
66.249.93.207	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	159
149.78.239.91	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	159
149.88.30.37	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	158
66.249.79.110	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	154
149.78.36.205	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	154
66.249.93.199	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	150
79.181.131.227	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.177.122.182	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
199.207.253.101	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	140
92.69.247.242	Netherlands	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	138
149.88.76.75	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	135

11-22-2015 to 11-23-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
168.235.64.163	United States	147.237.0.120		Multiple Unauthorized URL Access from 168.235.64.163	Block	2
82.166.162.73	Israel	147.237.0.120		Unauthorized HTTP Method	Block	2
168.235.64.163	United States	147.237.0.120		PHP Attempt	Block	2
46.19.85.157	Israel	147.237.0.120		Malformed URL	Block	1
46.19.85.157	Israel	147.237.0.120		Unknown HTTP Request Method 55 in URL	Block	1
82.166.162.73	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1
168.235.64.163	United States	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1213-he/miluim.aspx&	Block	1
46.19.86.247	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx&?â&Z	Block	1
95.86.66.127	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.aspx&sa=u&ved=0ahukewiq39psg6tjahvfvrokhsntaaqqfggi maa&sig2=d-au-iiuh5s1c5bk6qaaba&usg=afqjcnernh23git69bvqc8ggaxyqgn74qq	Block	1
176.12.137.137	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.behatsdaa.org.il	Block	1
82.166.162.73	Israel	147.237.0.120		Multiple Unauthorized URL Access from 82.166.162.73	Block	1

11-22-2015 to 11-23-2015