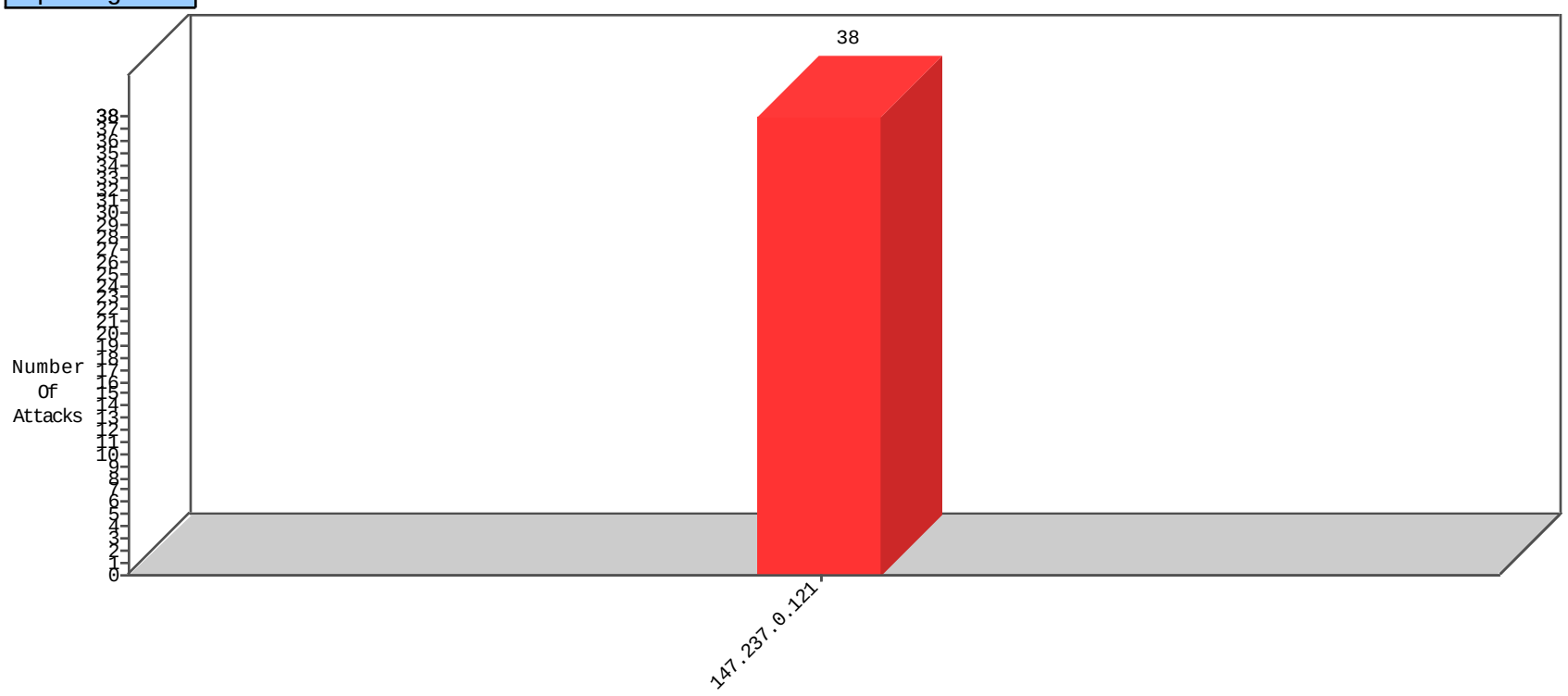
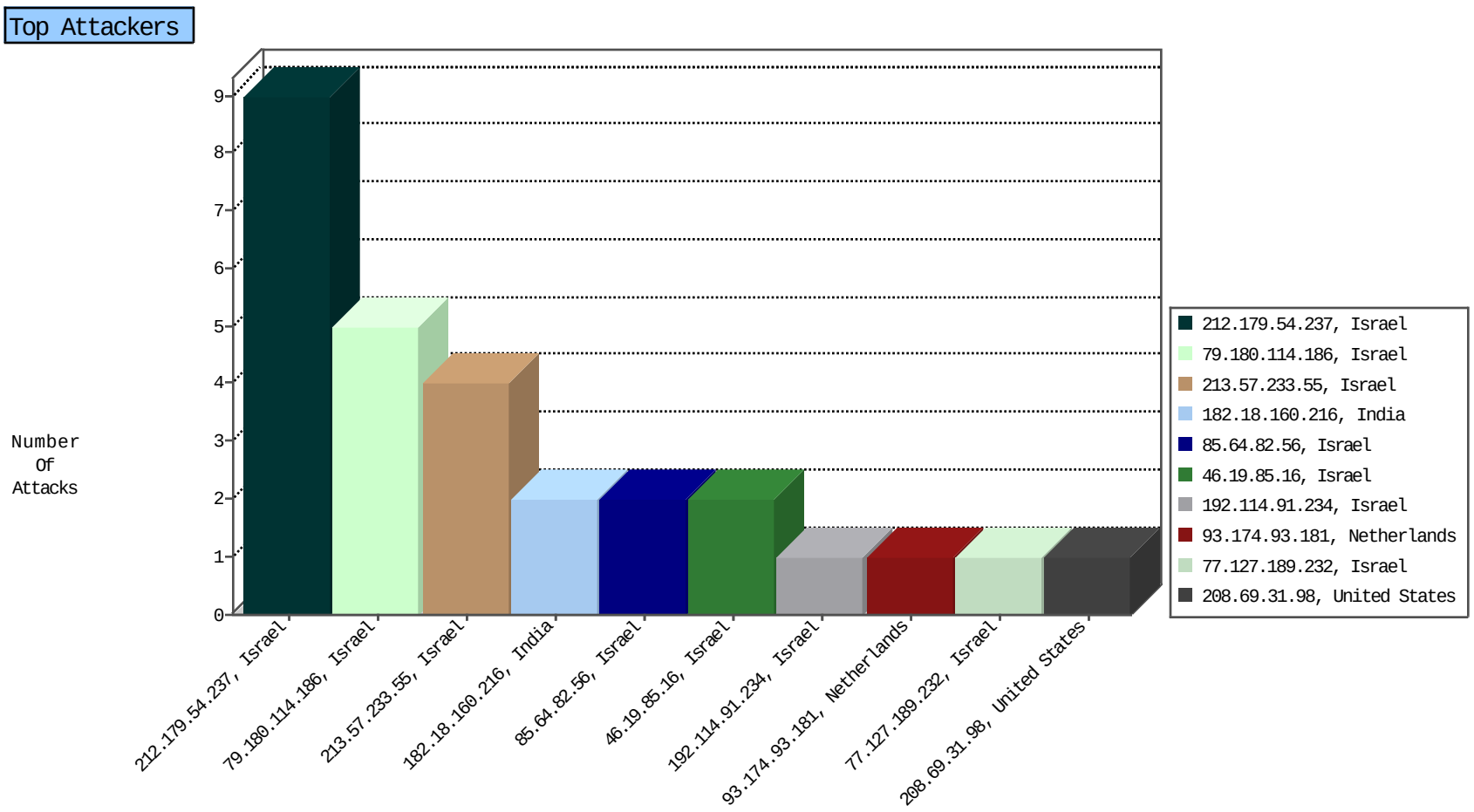
01-29-2016 to 01-30-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-29-2016 to 01-30-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	9

01-29-2016 to 01-30-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-29-2016 to 01-30-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
182.18.160.216	India	147.237.0.121		ET SCAN Potential SSH Scan	2
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
162.222.185.165	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
208.69.31.98	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
23.95.206.14	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
93.174.93.181	Netherlands	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
178.162.199.197	Germany	147.237.0.121		ET SCAN NMAP -sS window 1024	1
193.105.134.220	Sweden	147.237.0.121		ET SCAN NMAP -sS window 1024	1
222.186.34.94	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1

01-29-2016 to 01-30-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
31.168.89.122	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	450
149.78.225.127	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	392
149.78.240.70	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	386
68.180.228.25	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	352
149.78.25.176	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	318
149.88.106.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	246
149.88.126.229	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	171
149.78.131.176	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	99
149.78.252.185	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	84
149.78.20.96	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	82
149.78.225.8	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
68.180.228.168	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
149.88.72.71	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
68.83.252.122	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
149.50.77.180	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
149.88.143.245	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
149.88.219.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.78.51.107	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.78.233.80	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
46.120.244.192	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
88.128.81.17	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
149.88.197.235	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
173.234.233.203	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
167.206.154.30	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
149.78.8.248	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
84.228.199.94	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	18
79.183.154.215	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
79.182.205.65	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
149.88.193.6	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
66.102.9.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
94.230.86.136	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	12
52.90.80.35	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
188.120.148.107	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	10
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
131.253.35.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
80.246.137.122	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	9
94.230.86.136	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	8
31.210.187.172	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	6
94.230.86.221	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	6
108.161.241.20	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	6

01-29-2016 to 01-30-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.180.114.186	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	5
213.57.233.55	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	4
46.19.85.16	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
85.64.82.56	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
176.13.11.31	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.108.70.179	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.114.91.234	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
84.111.187.226	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
192.116.94.208	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
77.127.189.232	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1

01-29-2016 to 01-30-2016