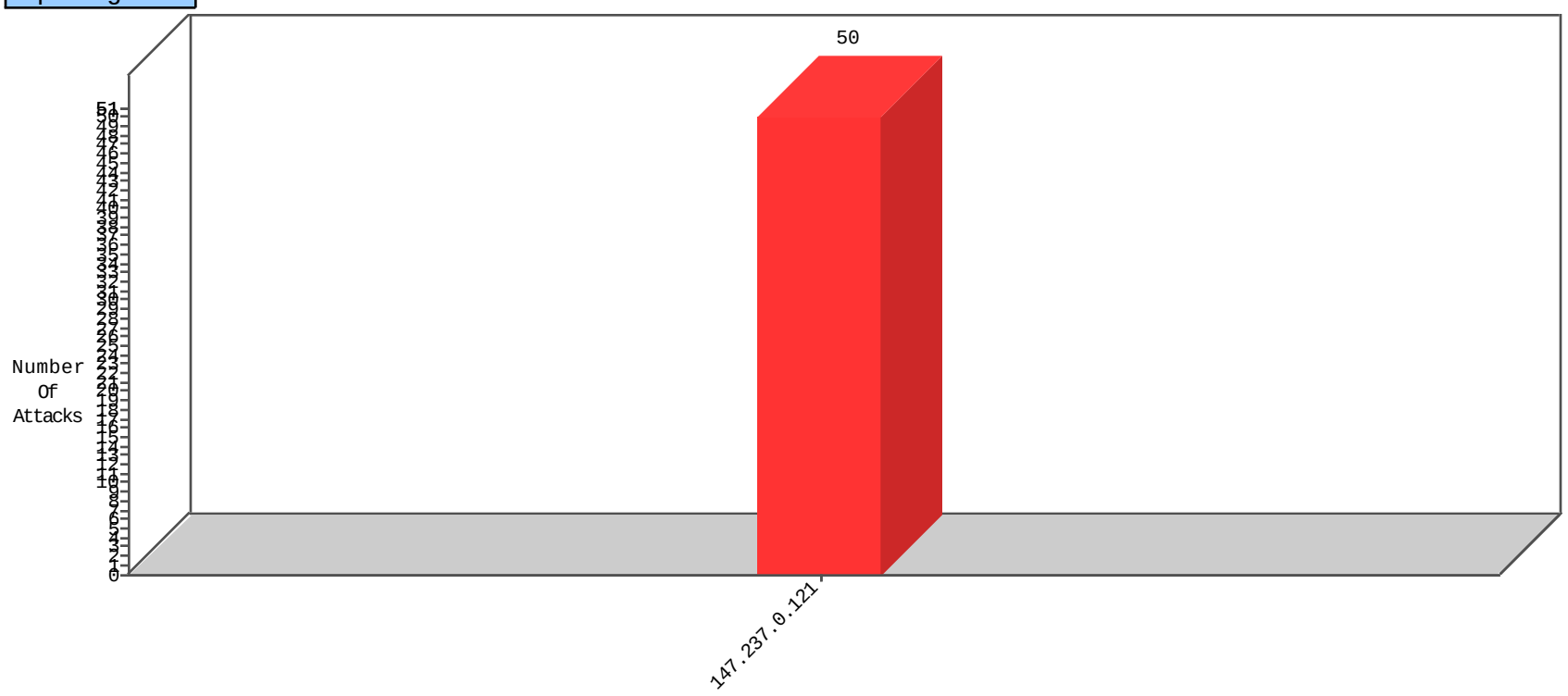
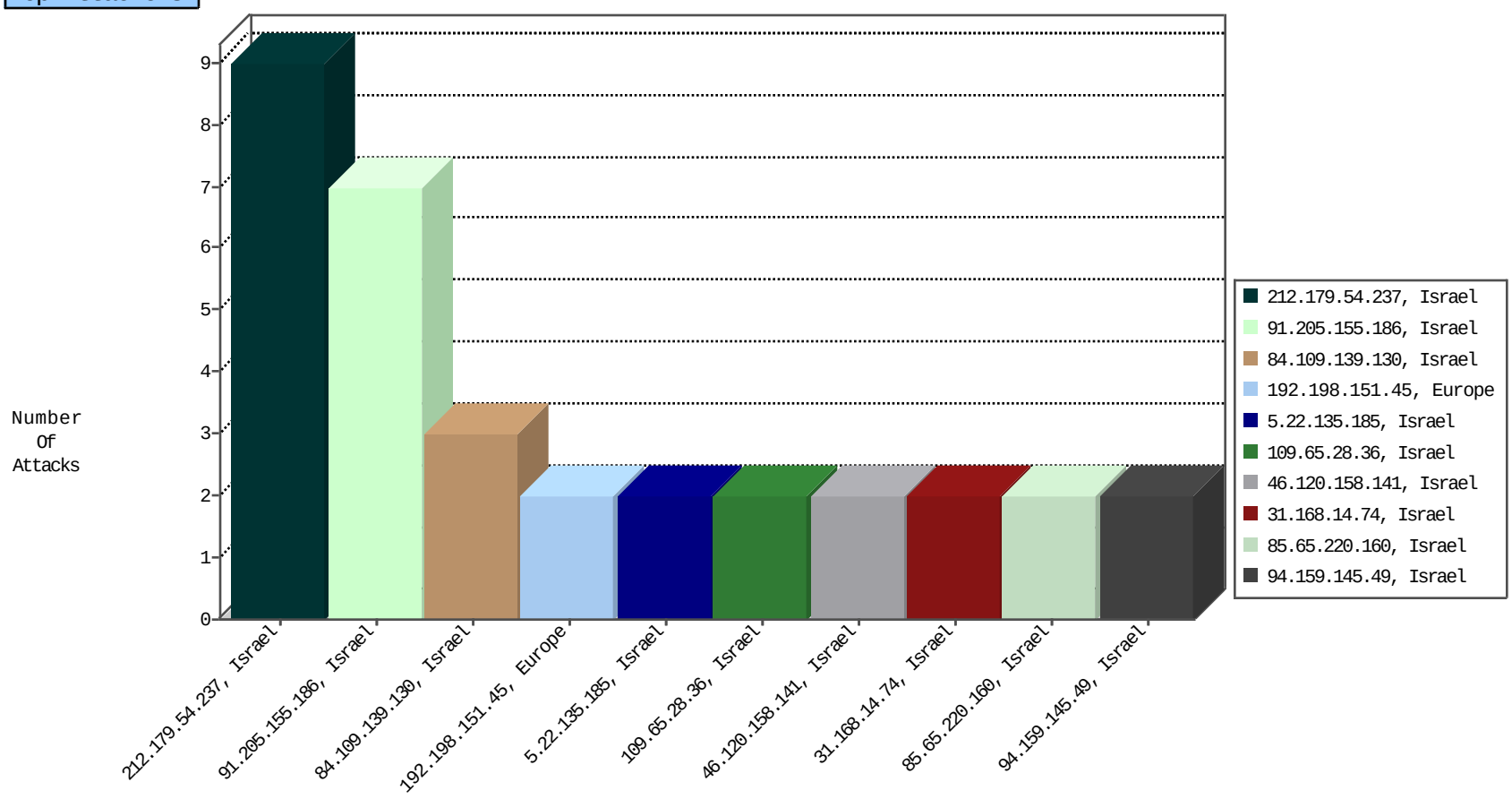
01-30-2016 to 01-31-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-30-2016 to 01-31-2016

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

01-30-2016 to 01-31-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-30-2016 to 01-31-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
218.1.31.135	China	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
193.201.227.104	Ukraine	147.237.0.121		ET SCAN Potential SSH Scan	1

01-30-2016 to 01-31-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
149.78.23.221	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	284
149.78.42.120	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	213
149.88.160.220	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	192
149.78.241.105	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	185
100.6.61.47	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
149.78.222.223	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	168
24.205.242.157	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
189.62.39.151	Brazil	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	160
149.50.80.108	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	150
149.88.242.30	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	110
79.179.182.28	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
149.78.241.99	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
149.88.148.111	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	103
149.78.255.176	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
149.88.127.48	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	86
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
93.73.2.157	Ukraine	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
149.78.22.158	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
149.78.230.122	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
110.77.249.209	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
149.88.233.249	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
149.78.169.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
149.50.71.237	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
149.88.70.252	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
80.101.6.54	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
149.88.13.227	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
149.78.42.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
149.78.229.80	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	29
149.78.46.3	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
149.88.83.108	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
176.119.123.113	Ukraine	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
54.172.254.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
149.78.196.198	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
149.50.95.40	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
149.88.142.117	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
52.91.148.120	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
209.126.117.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
31.210.186.144	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	9
37.46.38.247	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	9

01-30-2016 to 01-31-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
91.205.155.186	Israel	147.237.0.121		Suspicious Response Code	Block	7
5.22.135.185	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
46.120.158.141	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
85.65.220.160	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
31.168.14.74	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
2.52.24.40	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
94.159.156.46	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
84.109.139.130	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
46.120.95.142	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
194.90.129.28	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.181.178.13	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
95.86.121.179	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
84.109.139.130	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.76.103.245	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
94.159.145.49	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
84.108.180.147	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
5.29.95.197	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
109.65.28.36	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.65.28.36 (sigalgs DoS Attack)	None	1
46.121.247.2	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
213.57.233.55	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
94.159.145.49	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
84.109.139.130	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.109.139.130 (sigalgs DoS Attack)	None	1
109.65.28.36	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
85.250.34.30	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.128.48.166	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1

01-30-2016 to 01-31-2016