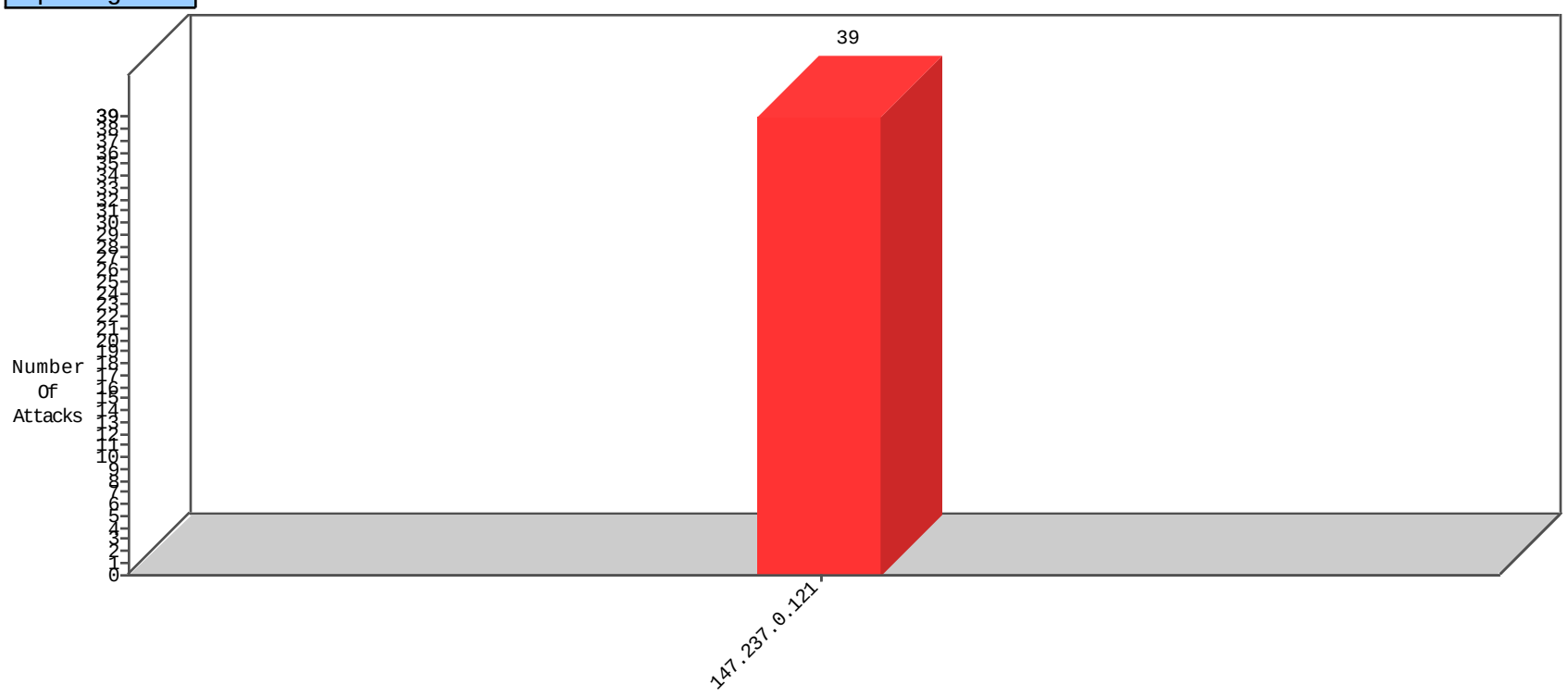
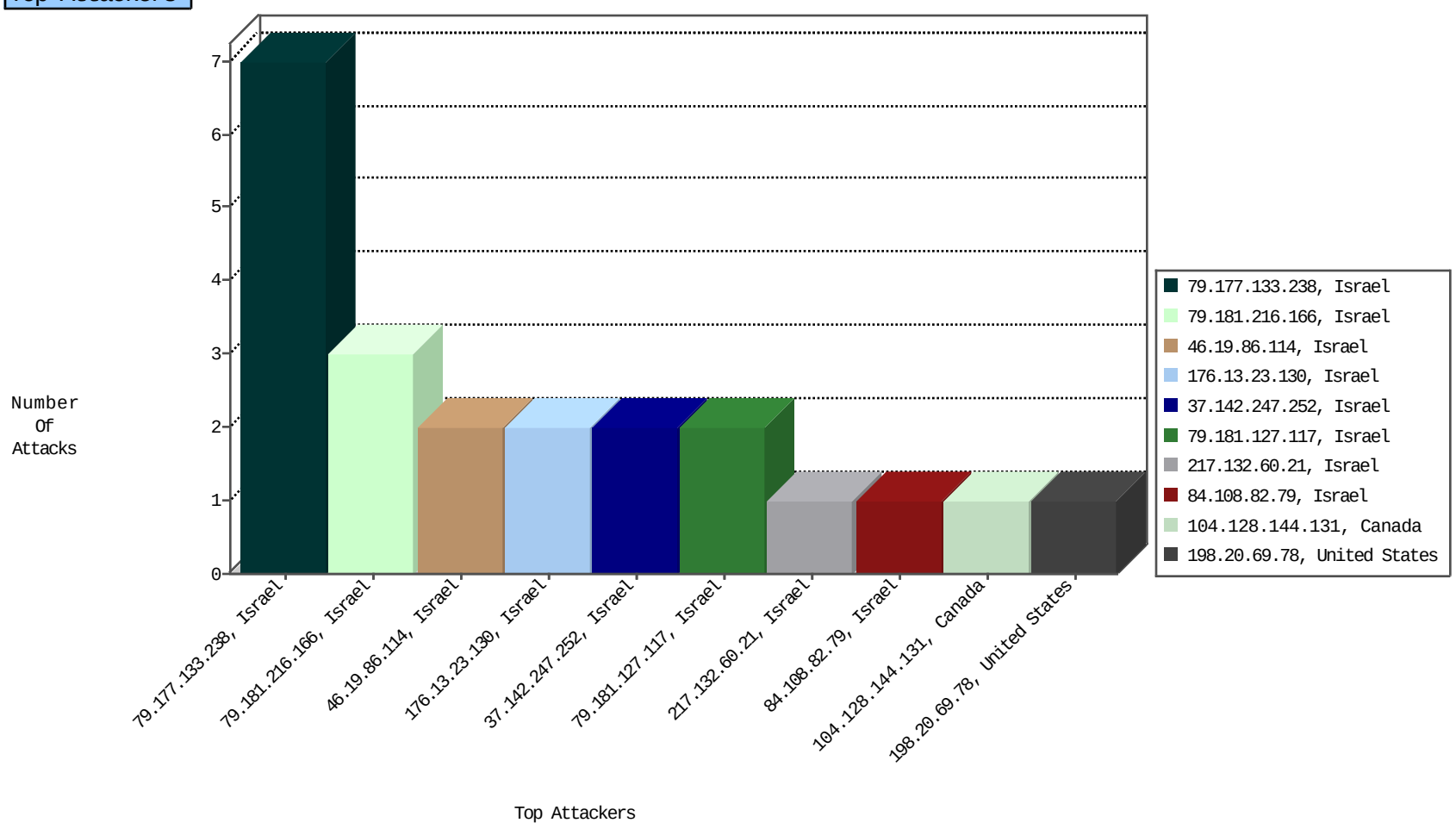
01-09-2016 to 01-10-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-09-2016 to 01-10-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count

01-09-2016 to 01-10-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-09-2016 to 01-10-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
41.215.130.239	Kenya	147.237.0.121		ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
104.128.144.131	Canada	147.237.0.121		ET SCAN NMAP -sS window 1024	1
122.234.232.82	China	147.237.0.121		ET SCAN Potential SSH Scan	1
185.130.5.247		147.237.0.121		ET SCAN Potential SSH Scan	1
52.90.147.148	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
62.210.203.114	France	147.237.0.121		ET SCAN Potential SSH Scan	1
107.191.63.157	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
131.100.80.110	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	1

01-09-2016 to 01-10-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
149.88.183.37	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4723
46.19.86.114	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1233
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1061
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1022
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	636
149.78.109.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	546
149.78.248.141	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	529
72.37.140.46	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	367
77.126.196.168	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
149.78.246.24	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	217
149.78.27.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	111
149.78.248.119	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.126.129	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	105
149.88.186.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
165.225.66.65	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	99
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
149.78.229.33	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
149.78.239.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
77.49.119.152	Greece	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.88.201.246	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
87.68.86.181	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
176.228.71.2	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
149.88.59.30	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
149.78.76.233	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
149.78.148.72	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
157.55.39.2	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	18
24.77.44.67	Canada	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
149.88.141.3	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
149.78.216.57	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
132.70.66.9	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
207.46.13.14	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
132.66.175.130	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	14
157.55.39.3	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
66.249.93.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
5.102.254.118	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	12

01-09-2016 to 01-10-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.177.133.238	Israel	147.237.0.121		Distributed Too Many of the Same Response Code (404)	Block	7
79.181.216.166	Israel	147.237.0.121		Suspicious Response Code	Block	3
176.13.23.130	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
83.130.115.195	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.19.86.114	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
217.132.60.21	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
95.86.120.85	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected A4ACC70A7E1F89A1701E16EDBE3F686E121EEB2497278961E7A10819F0D5D8F887B08B62944FA11AAF9BF1A0DFA43FE5CF721201E5CA373C497BA54ECB3ADBBECDD4D60AE326795476F8BA4D3A724A0F792DBF6AEFC8D8FCCCA7697EABAE6053A18CB03398605AE6935D54DE70163E3C722AA07FFB381B55CCD9B98496E14FE7, Observed 518A97C29D66BD4AC2B49C226C7A77DEFDD797DB8890EA4C55472D5D5F84FE7DEA5F49065CC2533B08FBBCB5F7CBEB5D5C2A8D56D508DD12D525A7E72AFF74094E29AD2DDAA82E5FDC107DC7AB092E706DF30BAF91CE38276D87667D142F70A1D98D28	None	1
79.181.127.117	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.181.127.117 (sigalgs DoS Attack)	None	1
2.54.13.117	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
185.120.125.16		147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
84.108.82.79	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.19.86.114	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
109.64.39.71	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.181.127.117	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.142.247.252	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 37.142.247.252 (sigalgs DoS Attack)	None	1
185.120.125.20		147.237.0.121		Suspicious Response Code	Block	1
84.108.223.139	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
176.13.23.130	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 176.13.23.130 (sigalgs DoS Attack)	None	1
37.142.247.252	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
198.20.69.78	United States	147.237.0.121		Unauthorized URL Access to 147.237.0.121/	Block	1
85.250.227.137	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
79.180.218.82	Israel	147.237.0.121		Distributed Too Many of the Same Response Code (404)	Block	1

01-09-2016 to 01-10-2016