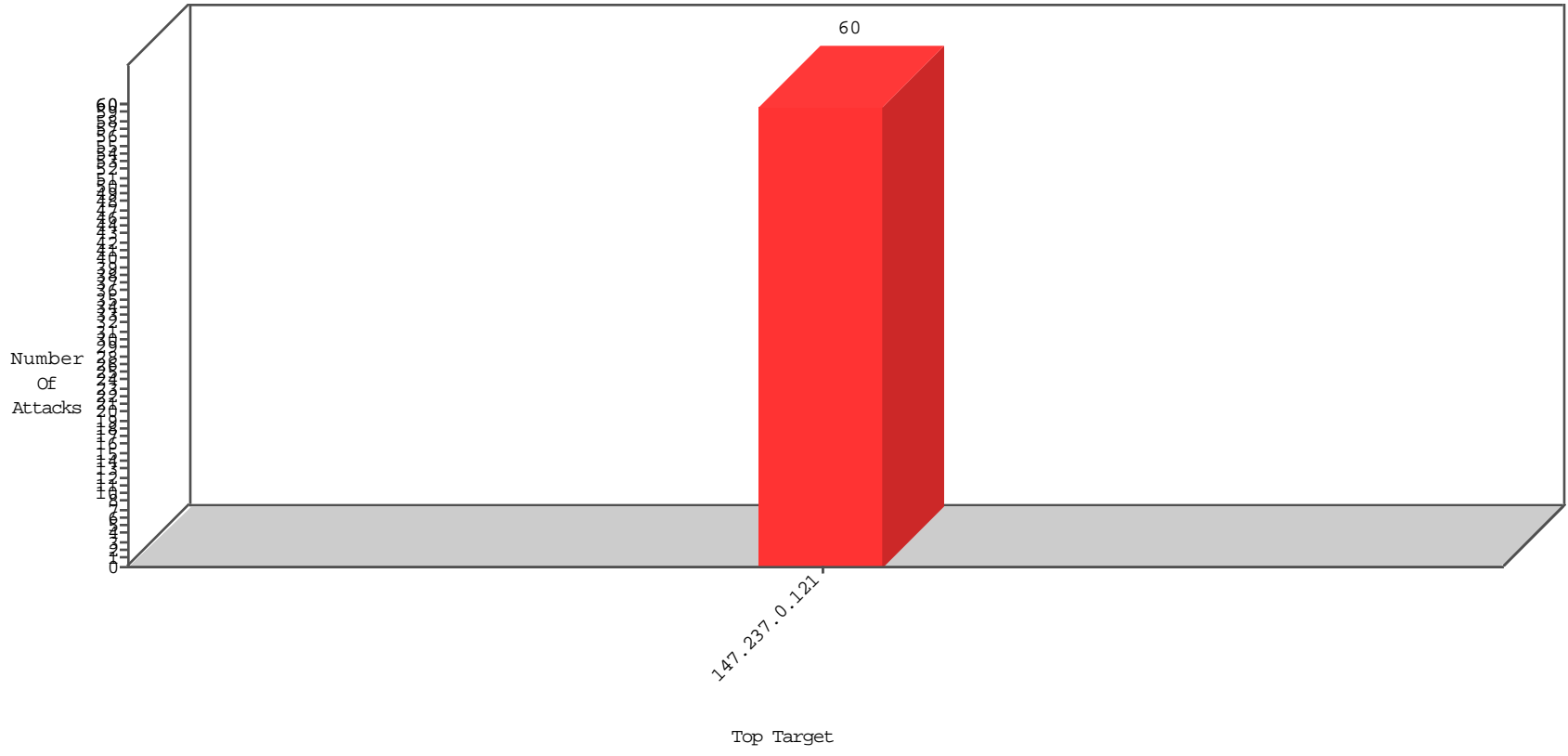


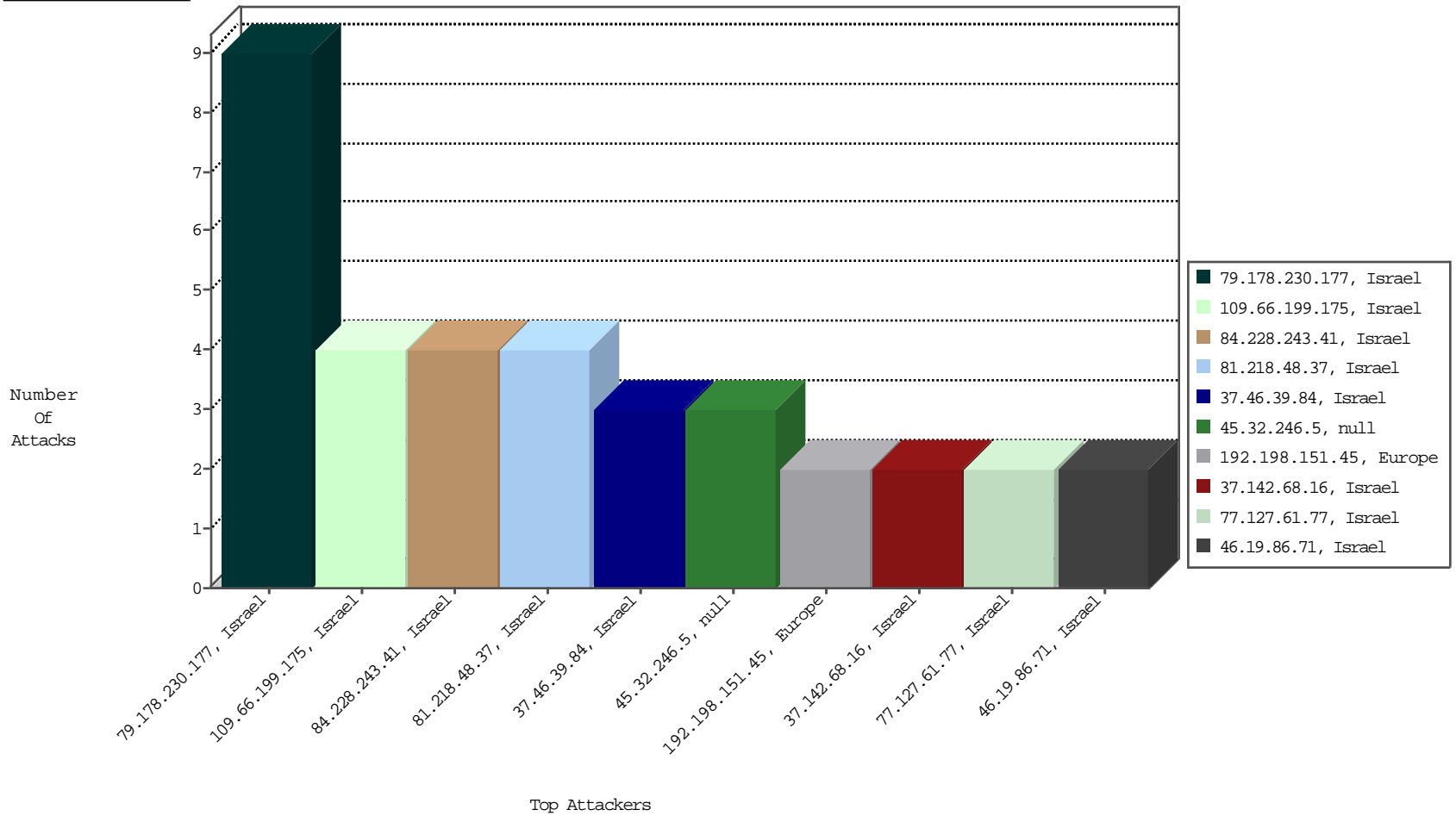
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



12-08-2015 to 12-09-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.178.230.177	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	9
45.32.246.5		147.237.0.121		Invalid TCP Flags	drop	BEL-Frankfurt	3

12-08-2015 to 12-09-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

12-08-2015 to 12-09-2015

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	2
200.199.196.74	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
66.249.93.149	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	2425
66.249.93.145	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	2198
66.249.93.153	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1840
66.102.9.74	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	227
66.249.93.145	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	224
66.249.93.149	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	223
66.249.93.153	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	216
149.78.240.163	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	204
192.116.48.38	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.140.80	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.102.9.97	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	140
149.88.179.53	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	137
149.78.215.20	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.88.207.54	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	88
66.102.9.87	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	85
80.246.136.76	Israel	147.237.0.121	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	81
149.78.233.91	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	70
79.177.123.231	Israel	147.237.0.121	drop	SAM rule	drop	60
217.69.133.253	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	53
66.249.93.254	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	52
217.69.133.21	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	51
66.249.81.251	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	44
79.182.61.154	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
192.146.6.2	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	40
138.134.102.15	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
58.11.36.50	Thailand	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	36
66.249.81.129	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	35
66.249.93.241	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	34
217.69.133.252	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	32
37.157.143.2	Bulgaria	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.191	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.249.93.219	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	28
217.69.133.248	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	27
46.19.86.134	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
66.249.93.215	United States	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	25
94.230.86.135	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	25
169.253.194.1	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.102.9.22	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.249.81.251	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.249.81.254	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.74.83	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.93.129	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	17
217.69.133.249	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	17
2.54.32.48	Israel	147.237.0.121	SYN Attack		reject	16
66.249.81.129	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	15
213.57.143.21	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
66.102.9.50	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	13
2.54.128.225	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.249.93.241	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	11

12-08-2015 to 12-09-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.66.199.175	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesNames in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	4
81.218.48.37	Israel	147.237.0.121		Suspicious Response Code	Block	4
37.46.39.84	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	3
46.121.68.148	Israel	147.237.0.121		Unknown Parameter ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	2
212.25.102.63	Israel	147.237.0.121		Suspicious Response Code	Block	2
84.228.243.41	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	2
46.19.86.71	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.127.61.77	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 77.127.61.77 (Open Mode)	None	1
37.142.68.16	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
213.57.90.18	Israel	147.237.0.121		Suspicious Response Code	Block	1
79.183.65.42	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
46.117.127.3	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesIDs in www.miluim-ishi.aka.idf.il/changeunit	Block	1
31.168.13.78	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
192.114.23.211	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
84.228.243.41	Israel	147.237.0.121		Multiple Illegal Parameter Encoding from 84.228.243.41	None	1
77.127.61.77	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.142.192.46	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
109.226.51.5	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
80.246.139.33	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.181.222.156	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
46.19.85.75	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
2.54.15.247	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.12.148.108	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.15.59	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.142.68.16	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
212.143.124.206	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/volunteeringbyage	Block	1
87.68.76.254	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
79.182.165.102	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
5.102.217.45	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
185.32.179.234	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.243.41	Israel	147.237.0.121		Illegal Parameter Encoding returnurl in www.miluim-ishi.aka.idf.il/login	None	1

12-08-2015 to 12-09-2015