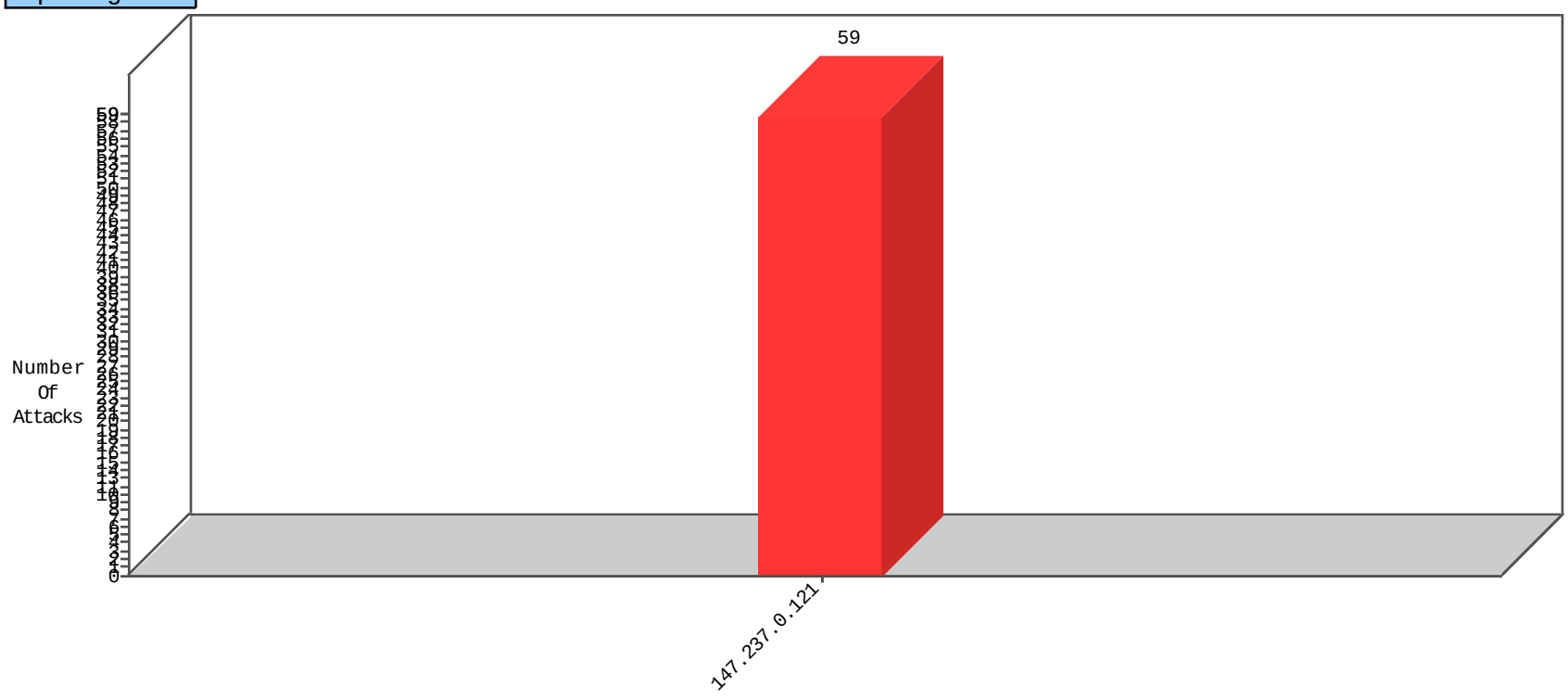
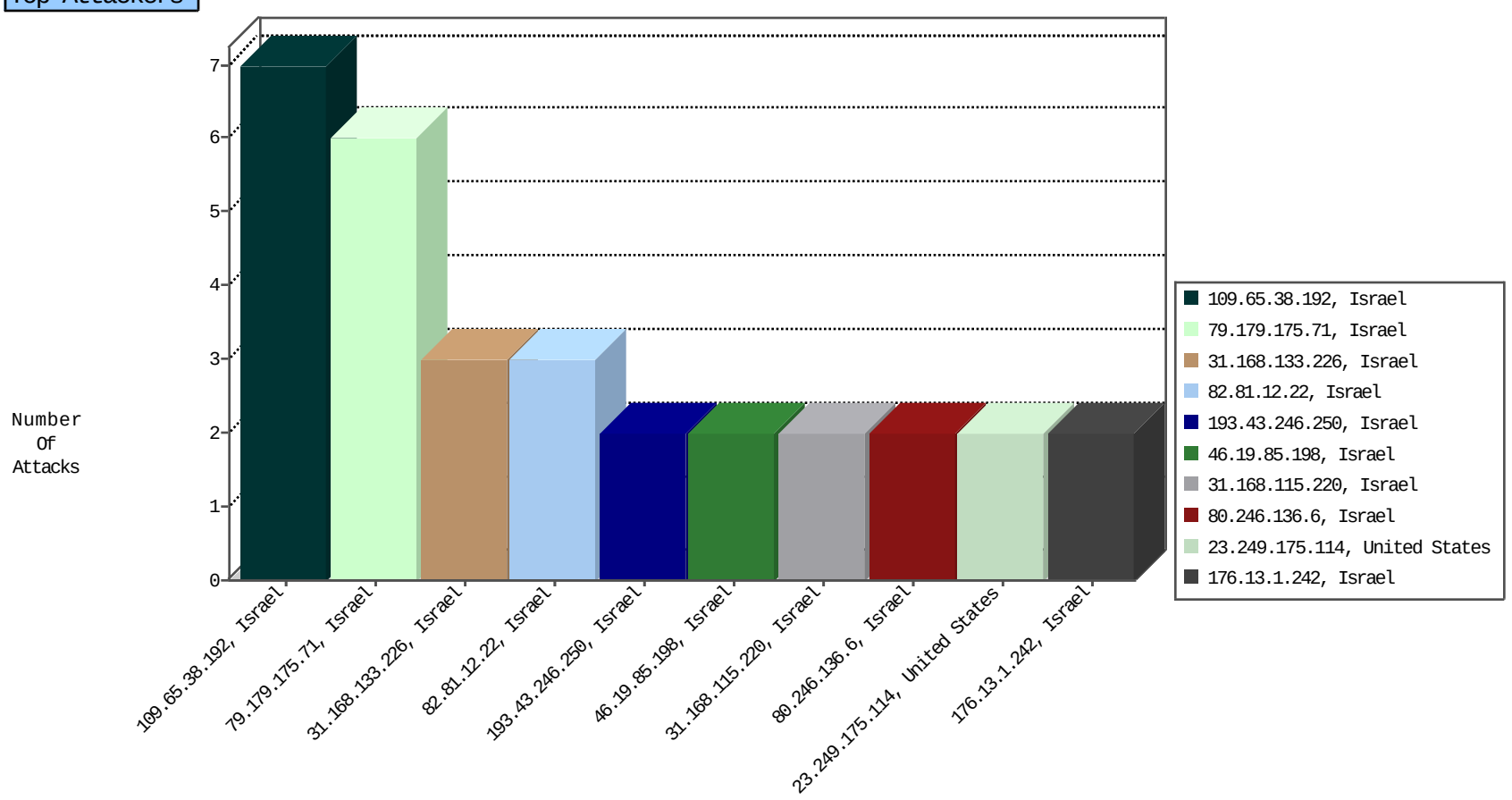
12-10-2015 to 12-11-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-10-2015 to 12-11-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.179.175.71	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	6
31.168.133.226	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
82.81.12.22	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

12-10-2015 to 12-11-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-10-2015 to 12-11-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
23.249.175.114	United States	147.237.0.121		ET SCAN NMAP -f -sS	1
138.94.34.136		147.237.0.121		ET SCAN Potential SSH Scan	1
23.249.175.114	United States	147.237.0.121		ET SCAN NMAP -sS window 2048	1
158.255.2.52	Russian Federation	147.237.0.121		ET SCAN Potential SSH Scan	1

12-10-2015 to 12-11-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1338
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1136
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1082
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	691
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	503
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	496
183.89.186.39	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	445
17.78.96.235	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	397
149.78.181.174	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	322
66.249.93.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	251
149.78.76.61	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	251
66.249.93.12	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	180
212.235.98.139	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	176
149.88.5.116	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	175
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	163
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	153
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	145
149.78.242.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	143
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
149.88.8.14	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	95
2.54.188.199	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	81
149.78.93.5	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
149.88.5.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
106.39.113.203	China	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
213.182.243.211	Austria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
82.166.198.101	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	45
66.249.75.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	41
2.54.191.18	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
82.81.81.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
82.81.81.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
52.6.144.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
82.81.21.10	Israel	147.237.0.121		Bad TCP sequence		monitor	34
149.78.233.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
149.78.224.236	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
70.32.45.67	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.249.74.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
212.179.5.3	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
31.154.151.206	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
66.249.93.15	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
109.64.55.22	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18

12-10-2015 to 12-11-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.65.38.192	Israel	147.237.0.121		Unauthorized HTTP Method	Block	7
31.168.115.220	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.198	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
193.43.246.250	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
5.22.134.55	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.1.242	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.144	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
213.57.54.107	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/volunteeringbyage	Block	1
109.65.202.230	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
82.81.21.10	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
46.19.86.179	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.13.9.27	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 769DACFC46937ED86D87544F7E979B75D3B944D32F70EB228F470B777A305FBF1AE91995C8DCEB455B132E0A7AFA1455BAAA67B04651ED3BD2032DB0C56D1DB77F87DAB9738458549867526EEBA0F4372E38FFB217A380A0337CDC64F77EC82C7DB0DFE0E5338AEFA8D64A44D45CE3D038CB9A7D21C9443007C7CC9401F106C8F6EC1CCE645A7FD0E084259F4E98F831DD951C61332B4E5029D9E23B71E7B511	None	1
104.236.122.221		147.237.0.121		Unauthorized URL Access to /	Block	1
80.179.244.189	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
2.52.39.45	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.67.108.37	Israel	147.237.0.121		Unknown Parameter v=7386392106594269504 in www.miluim-ishi.aka.idf.il/logincss	Block	1
85.64.244.63	Israel	147.237.0.121		Suspicious Response Code	Block	1
46.19.86.185	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.248	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
80.246.136.6	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 80.246.136.6 (sigalgs DoS Attack)	None	1
46.19.86.158	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
2.52.49.245	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
132.69.193.74	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
87.69.103.137	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.90.161.95	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.142.113.74	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.29.203.226	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
109.65.202.230	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.65.202.230 (sigalgs DoS Attack)	None	1
80.246.136.6	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.179	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.179 (sigalgs DoS Attack)	None	1
94.230.86.190	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
80.178.148.243	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1

12-10-2015 to 12-11-2015