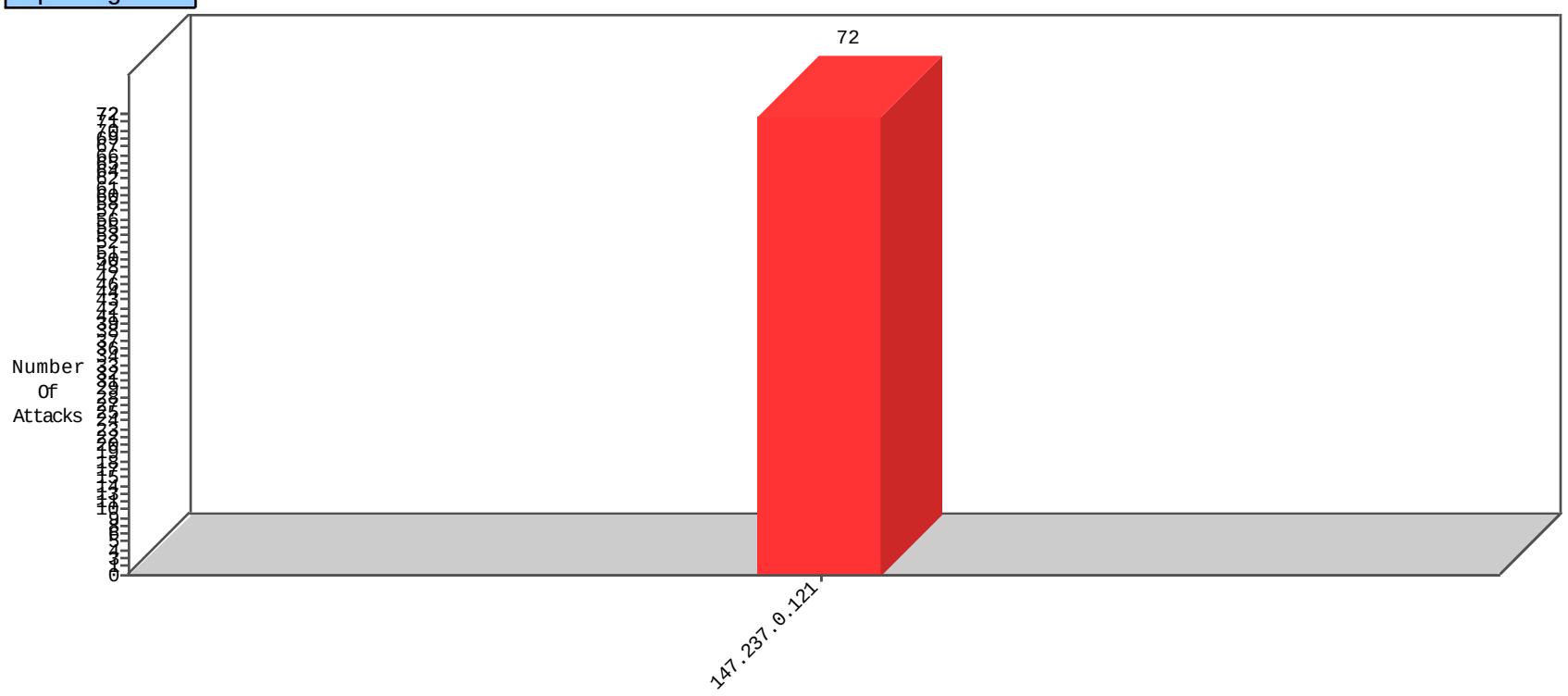
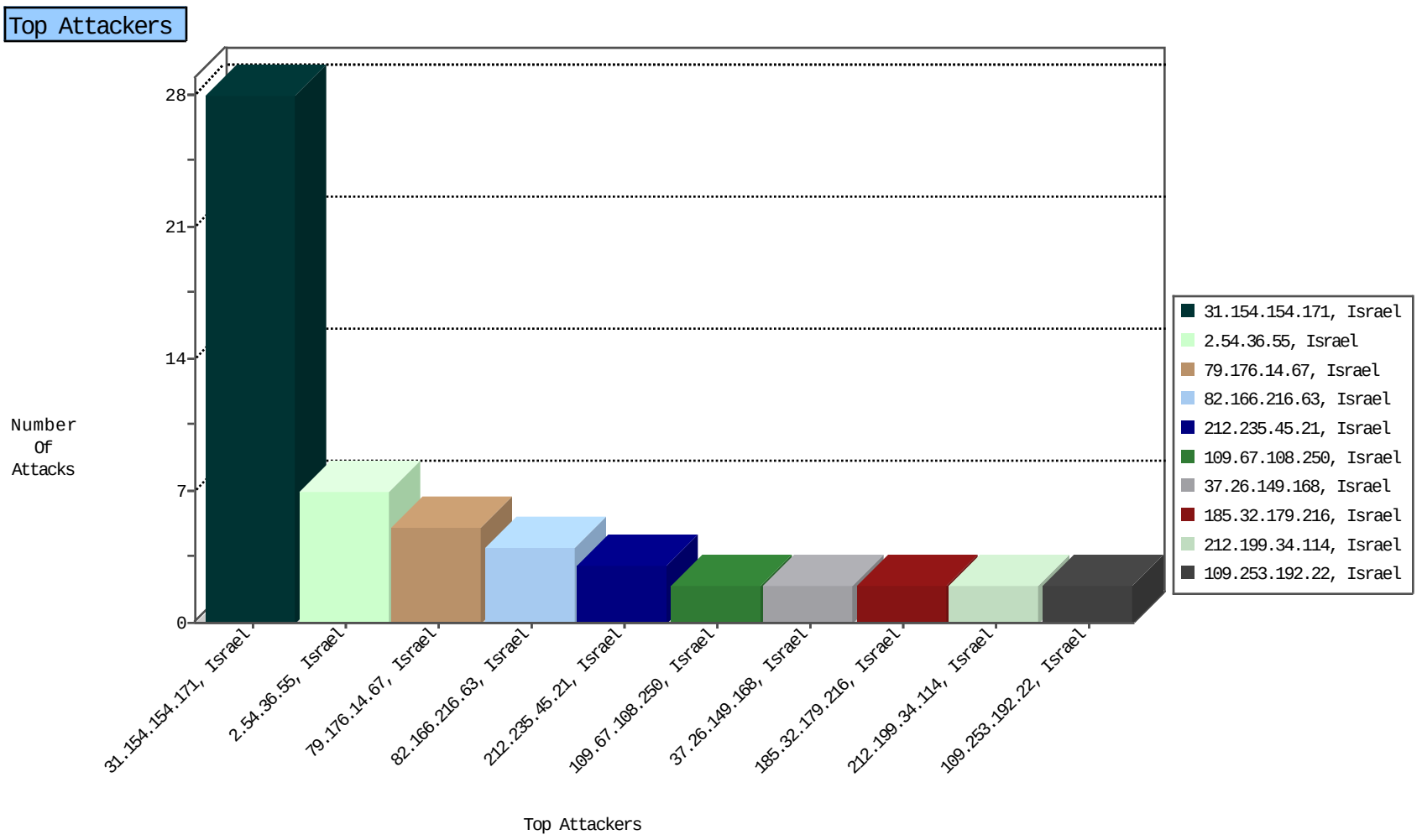
12-30-2015 to 12-31-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-30-2015 to 12-31-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
2.54.36.55	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	7

12-30-2015 to 12-31-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-30-2015 to 12-31-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
212.25.99.77	Israel	147.237.0.121		ET SCAN Potential SSH Scan	1

12-30-2015 to 12-31-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2566
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2405
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2106
108.171.128.172	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	590
134.191.232.69	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	565
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	300
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	286
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	198
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	191
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	174
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	167
207.46.13.164	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	133
62.0.101.97	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	99
149.78.20.76	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	98
62.0.101.97	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	97
144.132.68.73	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	81
157.55.39.178	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	65
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
149.88.20.106	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
157.55.39.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
149.78.183.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
69.203.154.223	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
222.152.66.223	New Zealand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
2.54.158.194	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
5.102.254.53	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
2.54.36.55	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
93.172.39.68	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
192.115.103.134	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	33
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
2.52.162.62	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	28
66.249.69.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
149.78.31.17	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
66.249.93.236	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
5.102.254.53	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	20
66.249.69.165	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
173.245.115.77	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.73.156	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.69.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
192.118.117.100	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
109.67.27.203	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	13
5.102.254.104	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	13
66.249.93.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
173.245.115.78	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
173.245.115.76	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
31.154.154.171	Israel	147.237.0.121		Suspicious Response Code	Block	28
79.176.14.67	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
212.199.34.114	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
109.67.108.250	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.216	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.235.45.21	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 212.235.45.21 (Unknown SSL Session)	None	2
79.176.14.67	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.176.14.67 (sigalgs DoS Attack)	None	1
37.26.147.233	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
212.235.45.21	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
109.253.192.22	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.253.192.22 (sigalgs DoS Attack)	None	1
82.166.216.63	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.85.209	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
2.54.8.38	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.76.98.28	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
93.157.86.33	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
79.176.14.67	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.26.149.168	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 37.26.149.168 (Unknown SSL Session)	None	1
213.8.204.7	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
109.253.192.22	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
82.166.216.63	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.197	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.150.196	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.26.149.168	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
82.166.216.63	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
62.0.101.97	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 18BB55D979639D65EC516A878F22CFC45304191925E231CAE6DE639D4A8FC40EDCA8AEC80D784E69C4026A59820602D05DDC900AD65CFAC7FA750EE7A983C356137D63CF87586F0C36773F3DC3C593811C7069F55C300B8D0524C8B8A6B73C0F89F75713C08E3B5FF7A0DE33744A340F532D2E9F3149F2E38A7BC8206EE05B713D9E611BC89CF057A64C7A893035031E4F321B7A5A23321186F266D82A6904F7	None	1
109.67.153.197	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/login	Block	1
82.166.216.63	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddAddressAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
37.46.42.100	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
192.115.177.203	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
83.130.115.227	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1