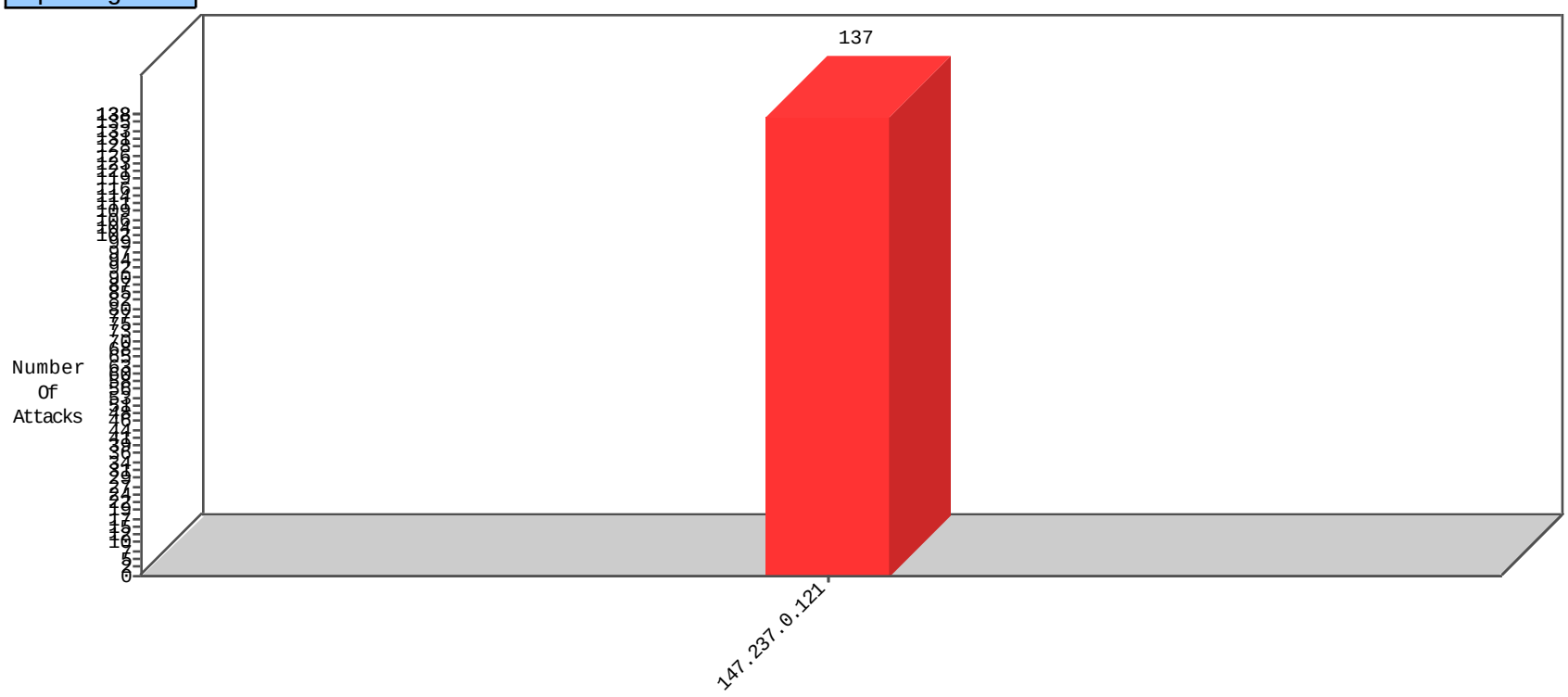
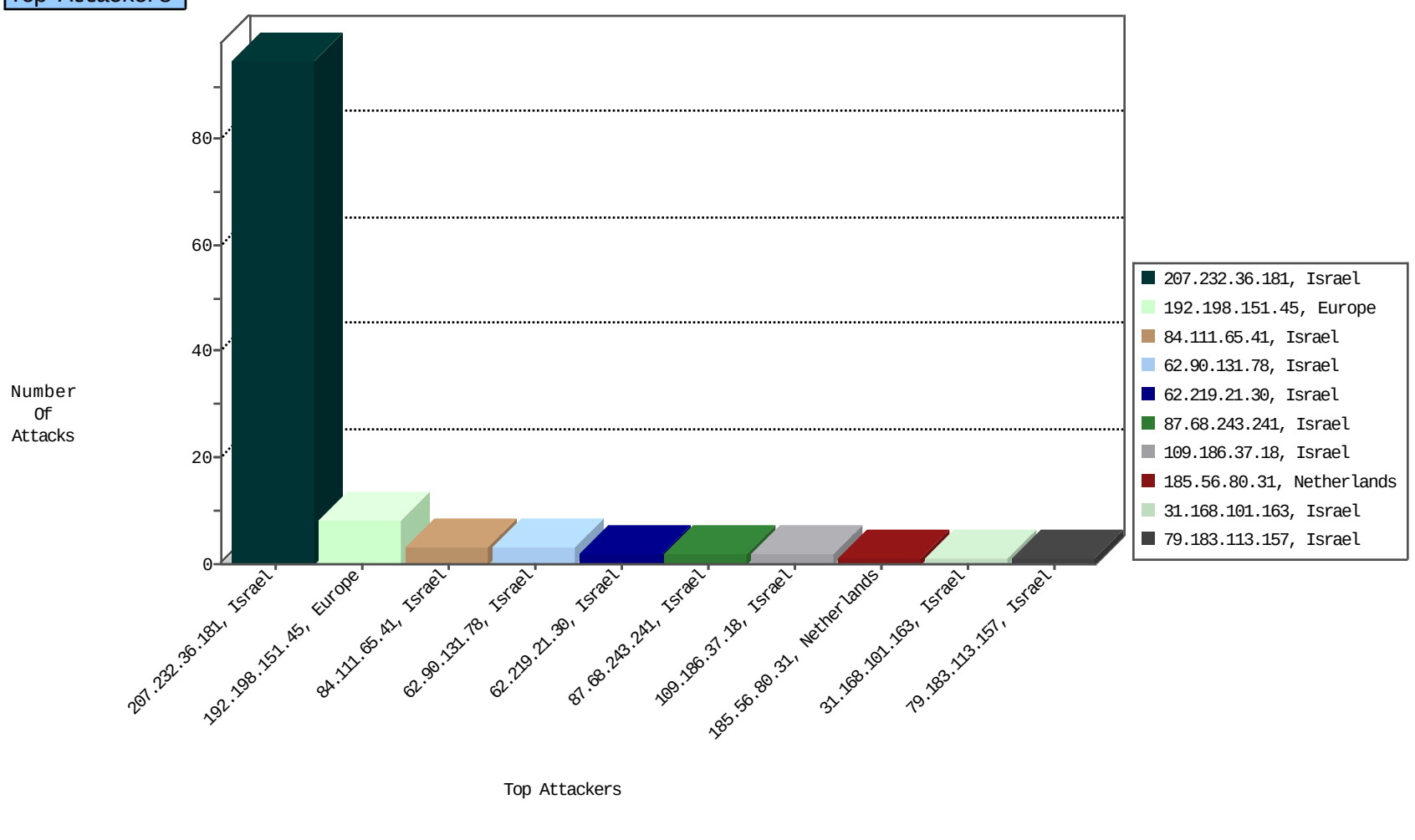
11-26-2015 to 11-27-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-26-2015 to 11-27-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
207.232.36.181	Israel	147.237.0.121		Anomaly-TLS-renegotiation-Cli	dest-reset	BBL-Israel	95
84.111.65.41	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

11-26-2015 to 11-27-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-26-2015 to 11-27-2015

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)	3
222.73.119.253	China	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
116.228.38.138	China	147.237.0.121		ET SCAN Potential SSH Scan	1
43.229.53.89	Japan	147.237.0.121		ET SCAN Potential SSH Scan	1
61.182.170.38	China	147.237.0.121		ET SCAN Potential SSH Scan	1
185.56.80.31	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1

11-26-2015 to 11-27-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3362
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2725
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2092
149.88.12.144	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	468
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	298
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	290
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	286
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	284
112.185.130.163	Korea, Republic of	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	262
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	213
149.78.221.136	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	200
201.163.222.179	Mexico	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	187
149.78.186.71	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	158
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	152
38.127.167.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	122
69.158.26.196	Canada	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	115
46.19.85.139	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
149.78.246.87	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	86
72.37.140.41	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
66.249.81.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
149.78.240.58	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
84.253.149.130	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	72
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	69
66.102.6.147	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
149.88.21.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
66.249.93.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
207.232.36.181	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	53
149.88.38.203	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
66.102.6.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
54.243.190.43	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
77.125.149.122	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.81.130	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
79.180.153.131	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	32
212.199.71.30	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	32
185.120.125.19		147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
185.120.125.19		147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
2.223.58.216	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
209.135.211.151	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
149.88.185.151	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
149.78.200.202	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.249.73.171	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
149.78.27.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
62.90.131.78	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	3
87.68.243.241	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
62.219.21.30	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	2
192.198.151.45	Europe	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
109.67.14.120	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
80.246.136.35	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
31.168.101.163	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
185.6.64.114	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
192.198.151.45	Europe	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
109.186.37.18	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.186.37.18 (Unknown SSL Session)	None	1
81.218.101.2	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.142.64.59	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
192.117.12.65	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
94.230.86.218	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
79.178.208.102	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
192.198.151.45	Europe	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
109.186.37.18	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
84.111.36.187	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
37.142.134.130	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
192.198.151.45	Europe	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected DEE6576508F6D4BC42078C28A9C48E152508EAB3737371E6EDF61CE55CB956B50C7E2A7757751C29355B47FEE8EEE565E89F6C5B4C8AB39E89D37326D3B9BA378F031C788B4DB94756071A22691E42C16C943CF438C8199B0E115894A2713016C4E5E10CD66A34E4E18C11D5CF112CA6A2ECF99C86372057D5D57529A82DA7E9, Observed 765CF640FC31BF473DAA51128CF23F20D8A6F7BFAFDDB9FF9DA6264FFFCA13228FE34816123DD4FAEB2EFDD7B12BD9CBED08E2214565872E8F17D9DBA79FFC8616D0F751472A8A49E573B5EB6EBF2E6259CAE3ABC5953573061B60F08E56E3C1D77214	None	1
95.86.92.59	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	1
79.183.113.157	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
31.168.10.91	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	1
192.198.151.45	Europe	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
109.226.60.144	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
84.228.161.200	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1