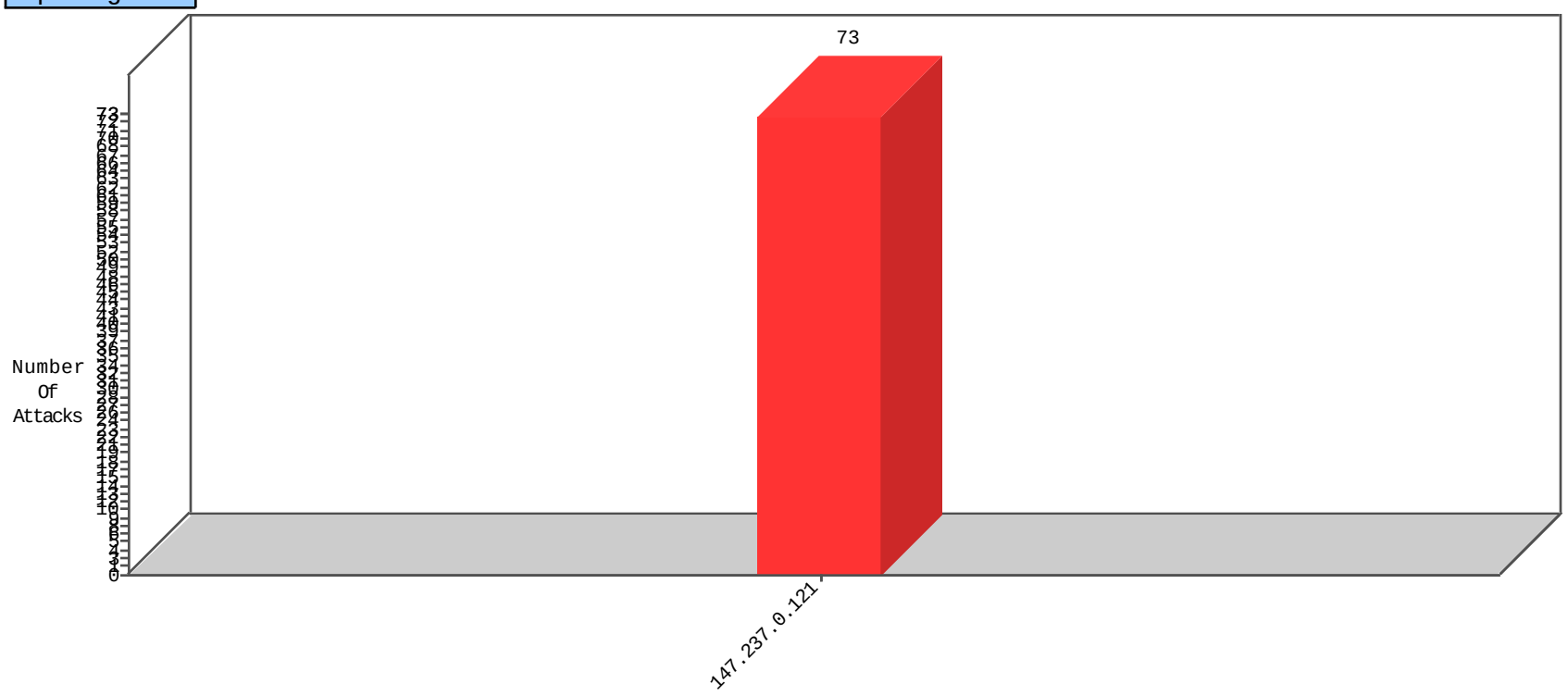
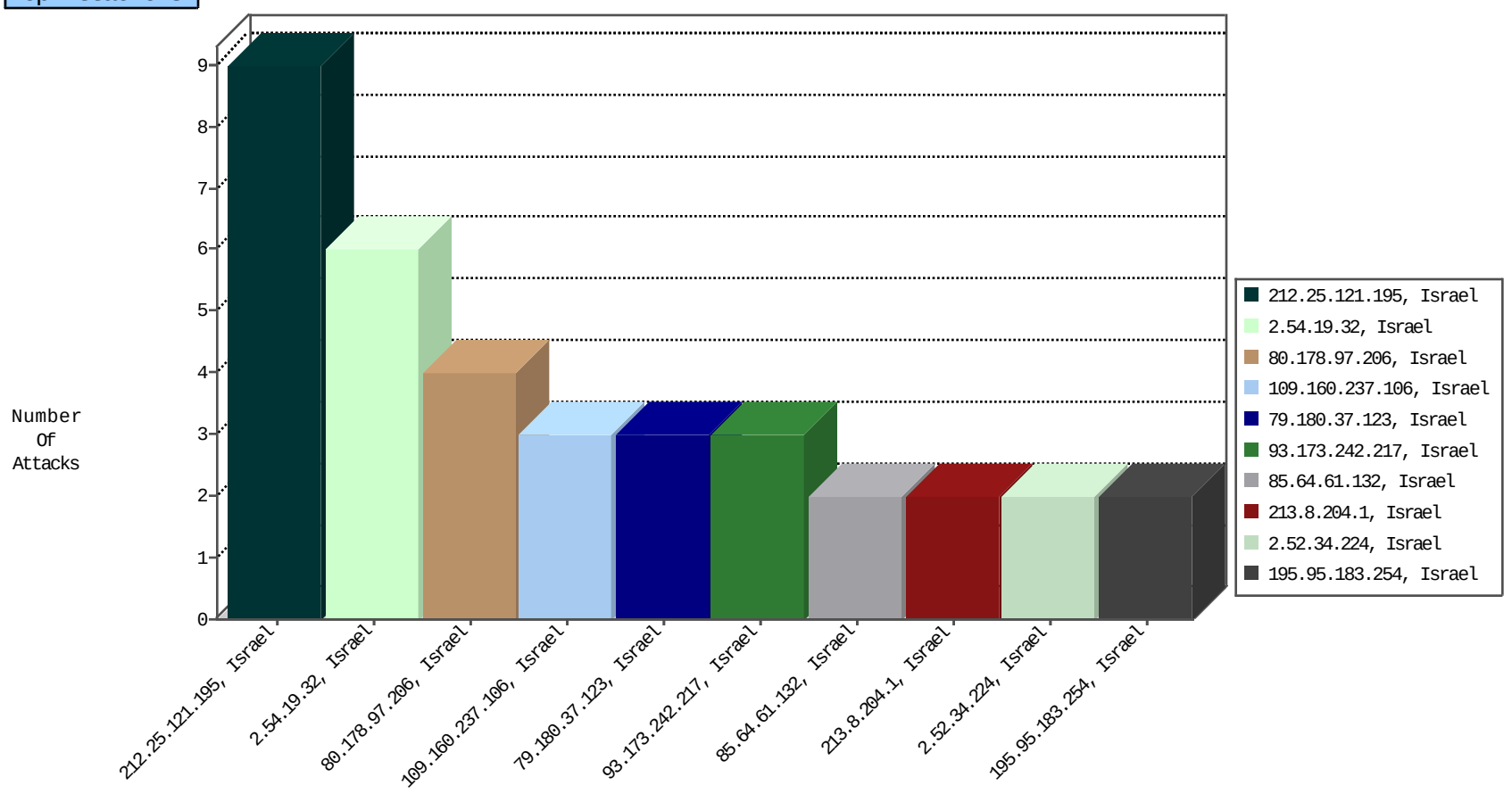
12-28-2015 to 12-29-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-28-2015 to 12-29-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.25.121.195	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	9
2.54.19.32	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	6

12-28-2015 to 12-29-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-28-2015 to 12-29-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
151.217.178.63		147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	2
210.73.74.202	China	147.237.0.121		ET SCAN Potential SSH Scan	1
210.117.121.60	Korea, Republic of	147.237.0.121		ET SCAN NMAP -sS window 3072	1
151.217.176.25		147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
192.198.151.44	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
210.117.121.60	Korea, Republic of	147.237.0.121		ET SCAN NMAP -sS window 1024	1
138.219.176.241		147.237.0.121		ET SCAN Potential SSH Scan	1

12-28-2015 to 12-29-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2925
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2792
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2425
64.236.4.3	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1253
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	278
54.172.21.120	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	270
46.19.85.205	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	270
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	236
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	219
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	211
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	208
40.77.167.25	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	178
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	165
2.54.19.212	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
157.55.39.199	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	133
83.170.100.194	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	130
2.52.27.73	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	115
2.52.27.73	Israel	147.237.0.121		SYN Attack		reject	113
157.55.39.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	110
66.102.6.84	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	98
207.46.13.46	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
46.19.85.16	Israel	147.237.0.121		Bad TCP sequence		monitor	81
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
49.65.223.211	China	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
46.19.85.16	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	64
15.90.166.11	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
15.90.162.12	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	58
108.13.8.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
66.102.6.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
82.166.57.226	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	52
62.90.70.70	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
74.94.135.197	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
95.35.0.254	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	44
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	37
2.54.19.32	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
185.3.144.16	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.146.67	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
66.102.6.90	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
2.52.27.73	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	31
2.52.27.73	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	31
149.88.95.207	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
66.249.69.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
2.52.27.73	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	27
149.78.230.148	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
84.95.211.33	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	25
199.203.226.21	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
109.65.11.81	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
185.32.179.138	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25

12-28-2015 to 12-29-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.160.237.106	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/changeunit	Block	3
79.180.37.123	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	3
93.173.242.217	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	3
213.8.204.1	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.148.72	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.156.88	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.9.192	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.178.97.206	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
195.95.183.254	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	2
85.64.61.132	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.80.133.133	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/changeunit	Block	2
2.52.34.224	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
37.142.129.130	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected DA73C62956AD582D1C4CA966E6499943E166CCFA274FBB0366B2669BB2757A13E2EFDCDF36753A98619478BC00D891D1BC5AE20B74B2983A9D0DBCC7E7C573CEEAE1594CE7223DE729703680C1D1A923A7C7B849DFA84EDA86FAA2B8143228B46EF92F620D4DEE3C876D4667FD709965543E35072D289B67AF28D51681165E1F, Observed 2ECB9515AAAE59F1D57CACAF30590EA1D5841D57A9E94C9E3A08F1AD8A6403FCF7BCE18042396FE83DECA45B49BCB39BEA83FC737DE378BE440F67ACE9A76654F0EBADAF608F275D958A66328259A2B59CD54B032362E8BEFC3E7DD3147EE69E335113	None	1
185.32.179.162	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	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
62.90.52.72	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
2.52.35.18	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
89.139.179.121	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 89.139.179.121 (sigalgs DoS Attack)	None	1
80.178.97.206	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.86.17	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.114.87.4	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
84.228.194.80	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.228.194.80 (Open Mode)	None	1
213.151.36.128	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
31.210.186.105	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected E04A5AB0E39E1B6813DE2271A81BAC9893B477E4989E14CEB2FDC9B8C0AECFED6A9876E8F11D5E27B1039839A19CC15885473B945FC86242104F67A6E3356E65EB2BF5C74065F24CCC7EF355BC7180895F4AEC66B438AD81C9B45BD91A1B1A411ED1D3DD20C82120EDCDE5B97722813533E00E32AD72DE5BC412C8587E67FC0B, Observed 1D64B2542DF2DA3563D9BF291633582EFE2C8C6660E3C37643531F459AD4DDF656FD9D10AD0250EEAAFFA6A4C9B0F6F21F68F2A67992A77486E2E57076F017D6E3127C1119801321D8AF98FB68791A75D95B5689EA0DF4732226BF44C8D1A5BAB02F21	None	1
89.139.179.121	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.65	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.65 (sigalgs DoS Attack)	None	1
109.253.199.159	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.181.93	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.26.148.151	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/changeunit parameter ctl00$ContentPlaceHolder1$Submit1	Block	1
176.13.22.119	Israel	147.237.0.121		Distributed Double URL Encoding	Block	1
46.19.86.65	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.76.119.220	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00$txtOldPass in www.miluim-ishi.aka.idf.il/personalsettings	Block	1
109.253.207.150	Israel	147.237.0.121		Distributed Double URL Encoding	Block	1
85.64.98.60	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
80.178.97.206	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 80.178.97.206 (Unknown SSL Session)	None	1

12-28-2015 to 12-29-2015