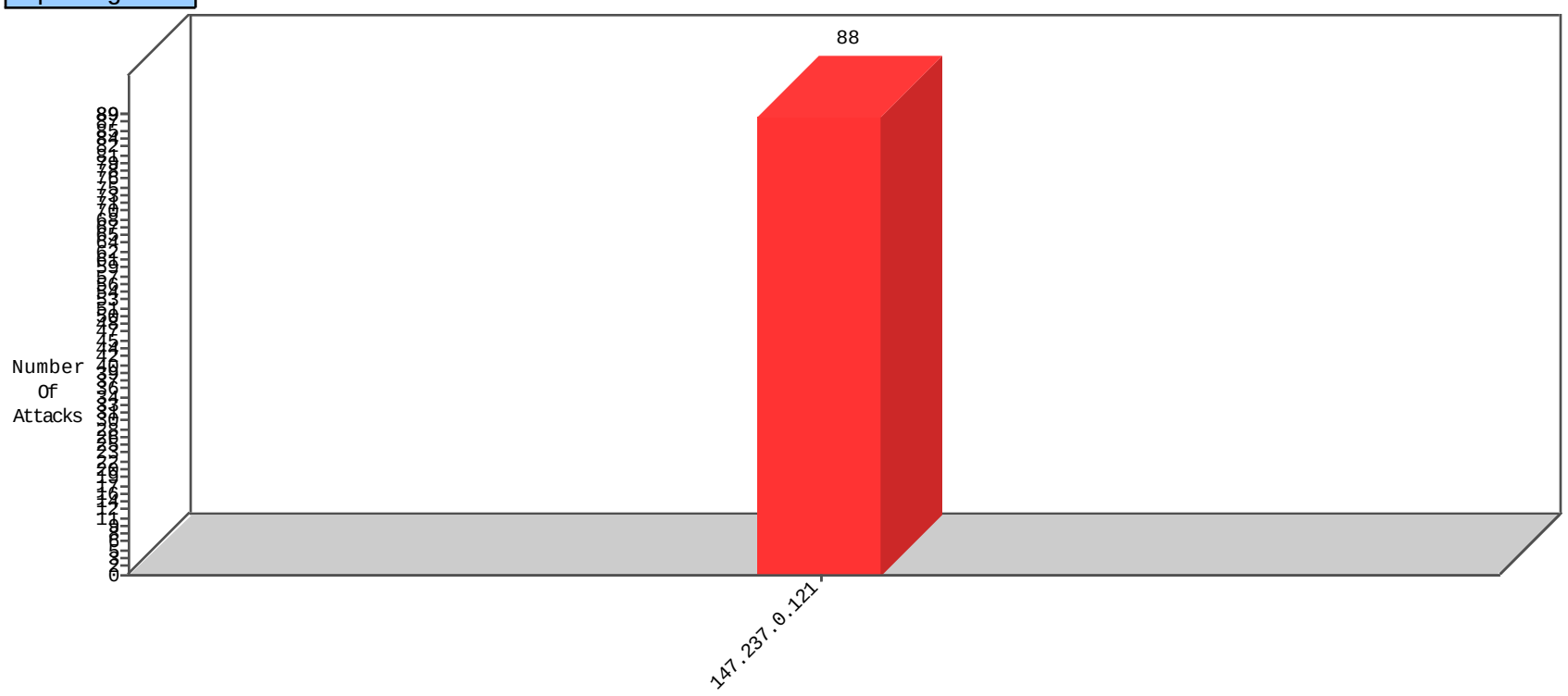
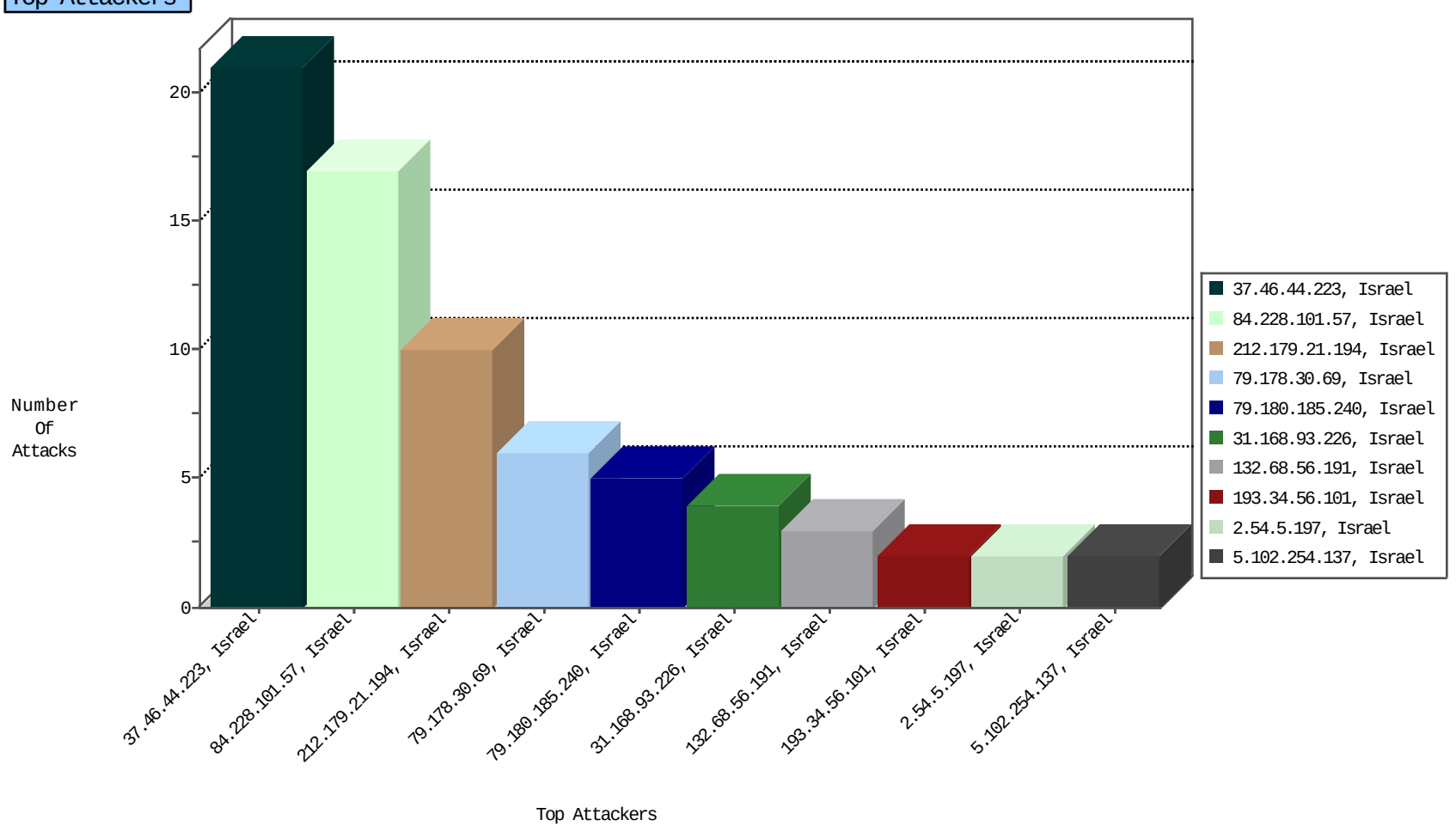
12-03-2015 to 12-04-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-03-2015 to 12-04-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.178.30.69	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	6

12-03-2015 to 12-04-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-03-2015 to 12-04-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
204.151.29.209	United States	147.237.0.121		ET SCAN NMAP -sS window 3072	1
204.151.29.209	United States	147.237.0.121		ET SCAN NMAP -sS window 4096	1

12-03-2015 to 12-04-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2621
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2605
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2564
149.88.11.130	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	832
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	356
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	322
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	291
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	286
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	219
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	160
2.52.7.58	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
149.88.111.47	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
176.151.99.29	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
149.78.234.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
149.88.226.62	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
149.78.35.188	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
40.115.5.243	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
149.88.66.5	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
84.228.101.57	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	40
149.88.38.197	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
31.186.228.29	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
31.186.228.95	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.249.93.215	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
2.54.138.115	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	27
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
69.171.231.224	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
66.249.80.42	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
149.88.132.190	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
109.186.152.2	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
120.19.135.181	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
157.55.39.115	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	23
143.127.2.4	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.249.93.247	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
194.90.134.227	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	21
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
212.179.28.66	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	20
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
79.180.185.240	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
94.230.84.116	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	18
149.78.87.204	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.93.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.0.121		Suspicious Response Code	Block	10
37.46.44.223	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddBoardExamsPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	6
37.46.44.223	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	6
37.46.44.223	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPermitFilesNames in www.miluim-ishi.aka.idf.il/valtamrequest	Block	6
31.168.93.226	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	4
79.180.185.240	Israel	147.237.0.121		Suspicious Response Code	Block	3
132.68.56.191	Israel	147.237.0.121		Parameter Type Violation __EVENTVALIDATION in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	3
193.34.56.101	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.46.44.223	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	2
37.46.44.223	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
213.8.129.147	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$fuAddDocsFiles in www.miluim-ishi.aka.idf.il/leaveinunit	Block	1
87.69.193.112	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
5.102.254.137	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.5.197	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.5.197 (sigalgs DoS Attack)	None	1
84.228.101.57	Israel	147.237.0.121		Multiple Unknown HTTP Request Method from 84.228.101.57	Block	1
84.228.101.57	Israel	147.237.0.121		Illegal HTTP Version	Block	1
79.180.185.240	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH)	None	1
192.198.151.43	Europe	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	1
84.228.101.57	Israel	147.237.0.121		Too Many Headers per Request - 69 Headers	Block	1
2.54.183.37	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Method from 84.228.101.57	Block	1
84.228.101.57	Israel	147.237.0.121		Abnormally Long Request method	Block	1
77.125.79.28	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
109.67.37.221	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/valtamrequest parameter ctl00$ContentPlaceHolder1$txtPermitFilesNames	Block	1
2.54.5.197	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.228.101.57 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
84.228.101.57	Israel	147.237.0.121		Malformed HTTP Header Line 24	Block	1
84.228.101.57	Israel	147.237.0.121		Unknown HTTP Request Method oÃ“[[#12]]rÃŸÂ’5Ã¢Â«I$Ã–sÂ?Â¢dApplications.aspx?_=1449168734612 in URL www.miluim-ishi.aka.idf.ilhttp/1.1	Block	1
2.54.183.37	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		Multiple Illegal HTTP Version from 84.228.101.57	Block	1
84.228.101.57	Israel	147.237.0.121		Illegal Byte Code Character in Header Value	Block	1
77.127.3.45	Israel	147.237.0.121		Unauthorized HTTP Method	Block	1
37.26.147.252	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.45.1	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		NULL Character in Header Name at [[#18]]4Ã€GXL•V`Â·Ã¦Ã–AÂ’[[#30]]Â¶Ã?;Â·Â®[[#31]]Ã†[[#19]]Â™qÂ¨-Â©UÂ²Ã¿Ã©vTÂšÂƒÃ™Ã›XÃºÂ-X[[#0]]ÃŽÃ©1EÃ‡e/Â–ÃƒÃ•~YÃ¥Â˜Â›*Ãª>ÂŒÃ€[[#23]][[#26]]ÃŸvÃ?Âœ½}[[#3]]SÂ¹ Y[[#22]]gÃ’Ã£6Â–Ã¸Ã”Ãœ4Â´Ã¾Ã¼^Â?BpA)ÃˆÃ°Ã‡?Ãˆh Â’Ã²FzPÃ¤2O[[#0]]sÃ–bZXÂ‡eGÂ¢EÃ‹Ã´ÂŒÂ§Â©[[#26]]Ã¹mÂ†Ã¸Â…Ã?Â¯p	Block	1
84.228.101.57	Israel	147.237.0.121		Malformed URL http/1.1	Block	1
82.102.169.113	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
87.69.109.149	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
5.102.254.137	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 5.102.254.137 (sigalgs DoS Attack)	None	1
84.228.101.57	Israel	147.237.0.121		Multiple Malformed URL from 84.228.101.57	Block	1
84.228.101.57	Israel	147.237.0.121		Illegal Byte Code Character in Method oÃ“[[#12]]rÃŸÂ’5Ã¢Â«I$Ã–sÂ?Â¢dApplications.aspx?_=1449168734612	Block	1
79.180.185.240	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.180.185.240 (Protocol violation (SSL_CONN_CLIENT_FINISH))	None	1
188.120.148.169	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
2.54.172.162	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.228.101.57	Israel	147.237.0.121		Multiple Abnormally Long Request from 84.228.101.57	Block	1
84.228.101.57	Israel	147.237.0.121		Abnormally Long Header Line request header name	Block	1

12-03-2015 to 12-04-2015