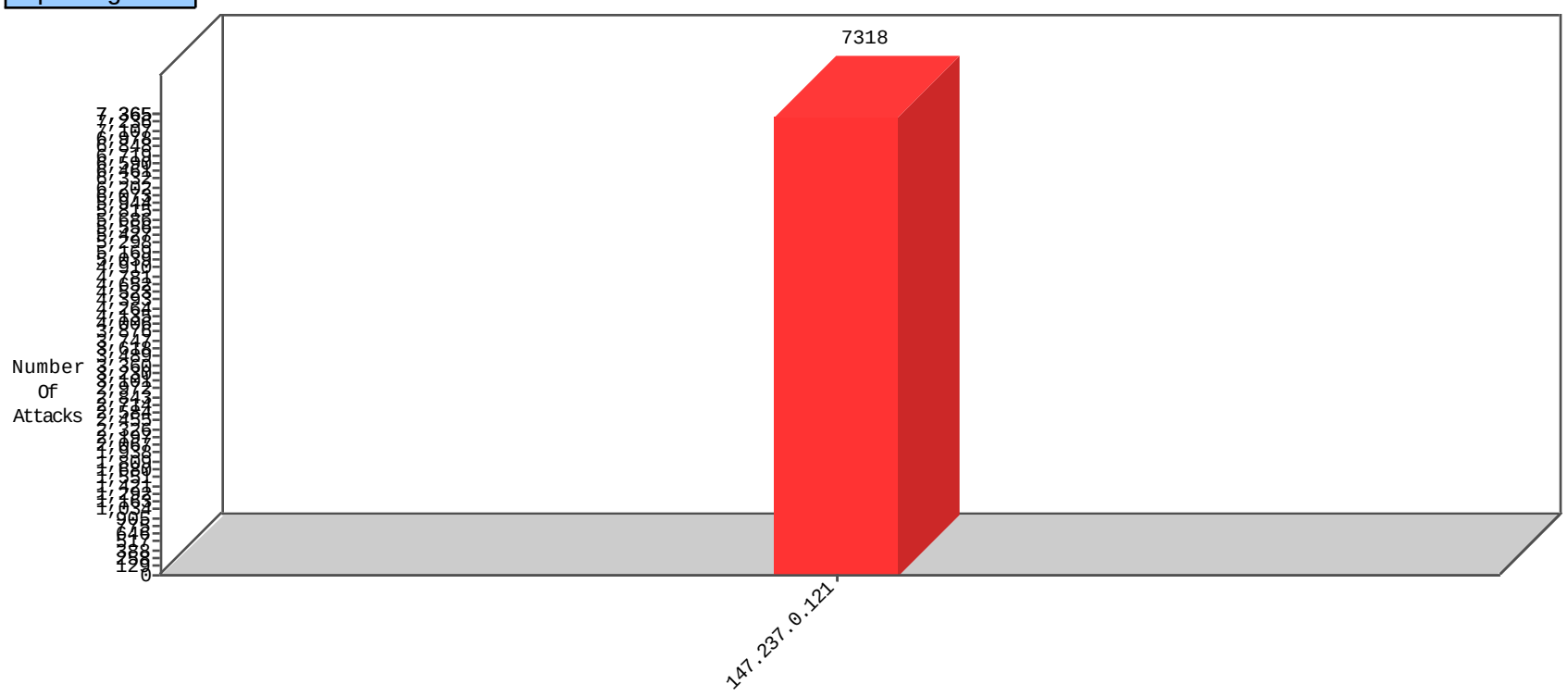
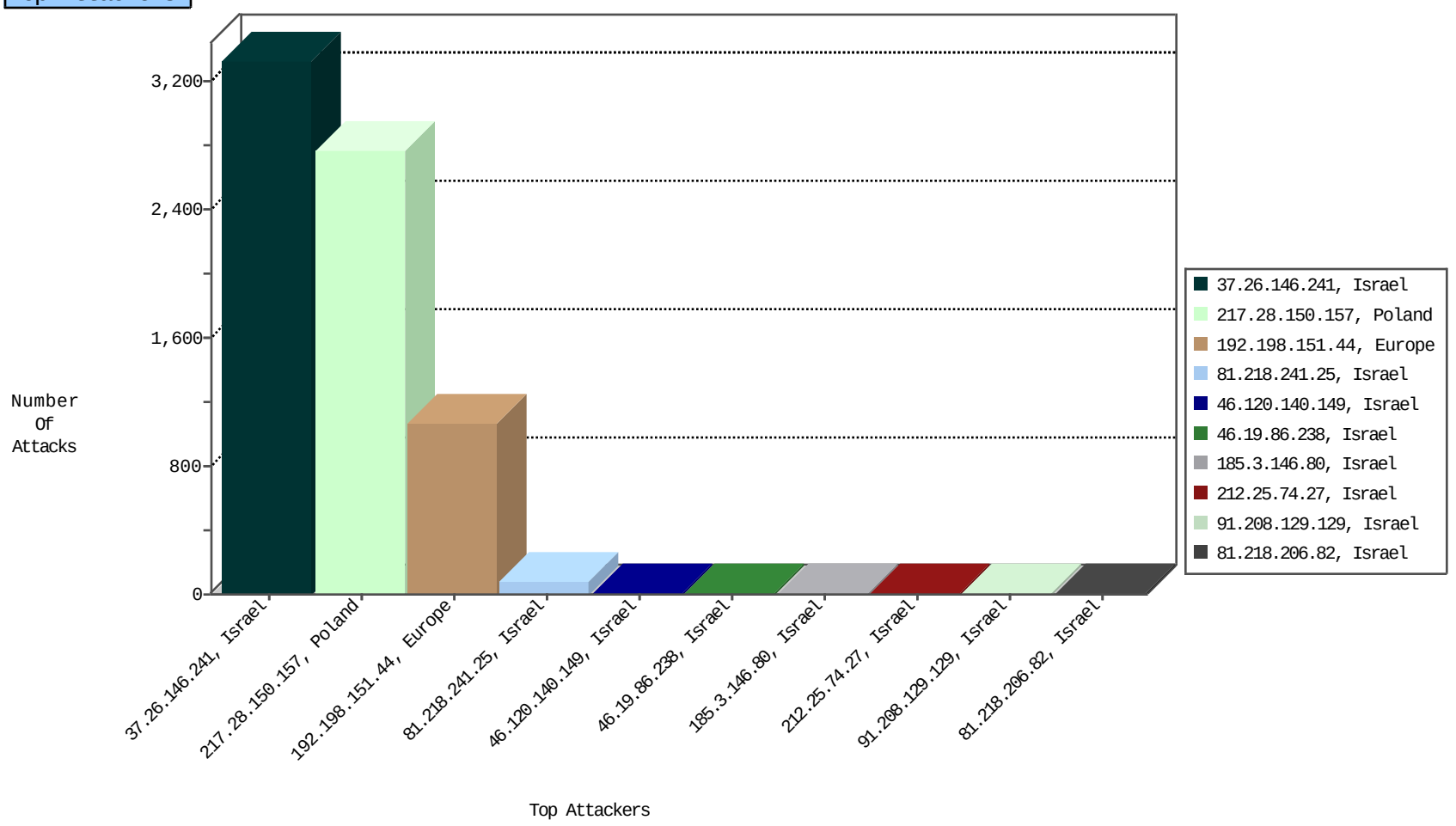
11-04-2015 to 11-05-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-04-2015 to 11-05-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
37.26.146.241	Israel	147.237.0.121		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	3336
217.28.150.157	Poland	147.237.0.121		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	2768
192.198.151.44	Europe	147.237.0.121		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1061
81.218.241.25	Israel	147.237.0.121		Anomaly-TLS-renegotiation-Cli	dest-reset	BBL-Israel	80
81.218.206.82	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
91.208.129.129	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
37.26.148.193	Israel	147.237.0.121		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1
46.120.140.149	Israel	147.237.0.121		Invalid TCP Flags	drop	BBL-Israel	1

11-04-2015 to 11-05-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-04-2015 to 11-05-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
46.120.140.149	Israel	147.237.0.121		POLICY-OTHER TCP packet with urgent flag attempt	10
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	3
187.60.247.195	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	2
188.138.9.51	Germany	147.237.0.121		ET SCAN NMAP -sS window 1024	2
194.63.140.74	Russian Federation	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
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1

11-04-2015 to 11-05-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3461
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2538
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2465
149.78.229.181	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1696
185.27.105.190	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	954
149.78.99.215	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	503
149.78.250.152	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	501
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	287
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	283
149.78.36.17	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	265
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	232
149.78.220.184	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	201
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	148
149.88.72.186	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	145
2.54.45.77	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
84.229.134.30	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.180.14.241	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.139.115	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.148.175	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
46.19.85.112	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
186.192.21.211	Brazil	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	110
109.65.191.34	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
2.54.165.233	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
66.249.93.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
2.54.185.156	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
2.54.11.219	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
66.249.81.235	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
149.78.32.34	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
217.69.133.252	Russian Federation	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	48
66.249.93.241	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
66.249.67.174	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
207.46.13.77	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
199.203.61.109	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	46
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
149.88.79.12	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
131.204.254.88	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
149.78.148.43	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.93.247	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
2.54.155.0	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
82.81.23.71	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
206.71.229.194	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
149.88.41.147	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
66.249.81.238	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.93.220	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.19.86.238	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	9
212.25.74.27	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	5
185.3.146.80	Israel	147.237.0.121		Multiple Unauthorized URL Access from 185.3.146.80	Block	4
185.3.146.80	Israel	147.237.0.121		PHP Attempt	Block	4
2.54.167.124	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
46.121.235.241	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
84.95.214.60	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
46.116.172.102	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
80.246.138.38	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
37.26.148.194	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
212.150.177.204	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
109.64.24.53	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1355-he/miluim.aspx	Block	1
5.28.128.242	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
82.166.81.221	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.19.85.148	Israel	147.237.0.121		Distributed Unknown Parameter on www.miluim-ishi.aka.idf.il/smsverify parameter ctl00$ContentPlaceHolder1$txtCaptcha	Block	1
213.8.21.71	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.66.135.63	Israel	147.237.0.121		Distributed PHP Attempt	Block	1
79.181.176.111	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.181.176.111 (Open Mode)	None	1
37.26.146.152	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 8169D92AB7E959EE4D030BB64132DEF481086D82BFBC34FD47B93F0BFC45DB3FFAA683740572BF1F698F444ECCE568923924F03A3CCD22AAA8CE946AB824D625D115A73EEEF5C88C268F1D7AAD7D6C86DCAB92EA06D018A5B4343C5017301A02BC2D4021D71F04CD9C7C1CF11116DC19544099A4245A65F9639D9B58586ABBA1, Observed 770DAD6213F595BF4A772E07ACD985E2B583959B38FA25A0D6F8F299C79BC6AAC839A693AF10F75099DFC995550758AB4D91563E30DF9B7A1E7A8D836363C30EF5B1780356841FA9B2BD4EF579BF3C21CF23DEE43840586B018E684BDEF7C67FD2041E	None	1
192.115.92.55	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
83.130.101.14	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
2.54.38.14	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.66.135.63	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ajax/pages/fan_status.php	Block	1
79.181.176.111	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.26.147.192	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 7014918550FF93D39678613477CC5B8495B7954D5B8C5D139F582328EE0171B4B298DAF465B032CDA50271AB85EA615D38B5401D59BFBAEBE74D7923A2B8FBEE89F9213C86A49D57AEE57EBF5B8E4109682E20829B74661A312B3CF2253F402A15A4DB20BA0935C477CFBFB51A867769C888DE96B2145431BF7CFB55D32EEEABED3FBEDEF733E7AC00862843B2254F8A3E375819E3CAC9DDD257315000C66F02	None	1