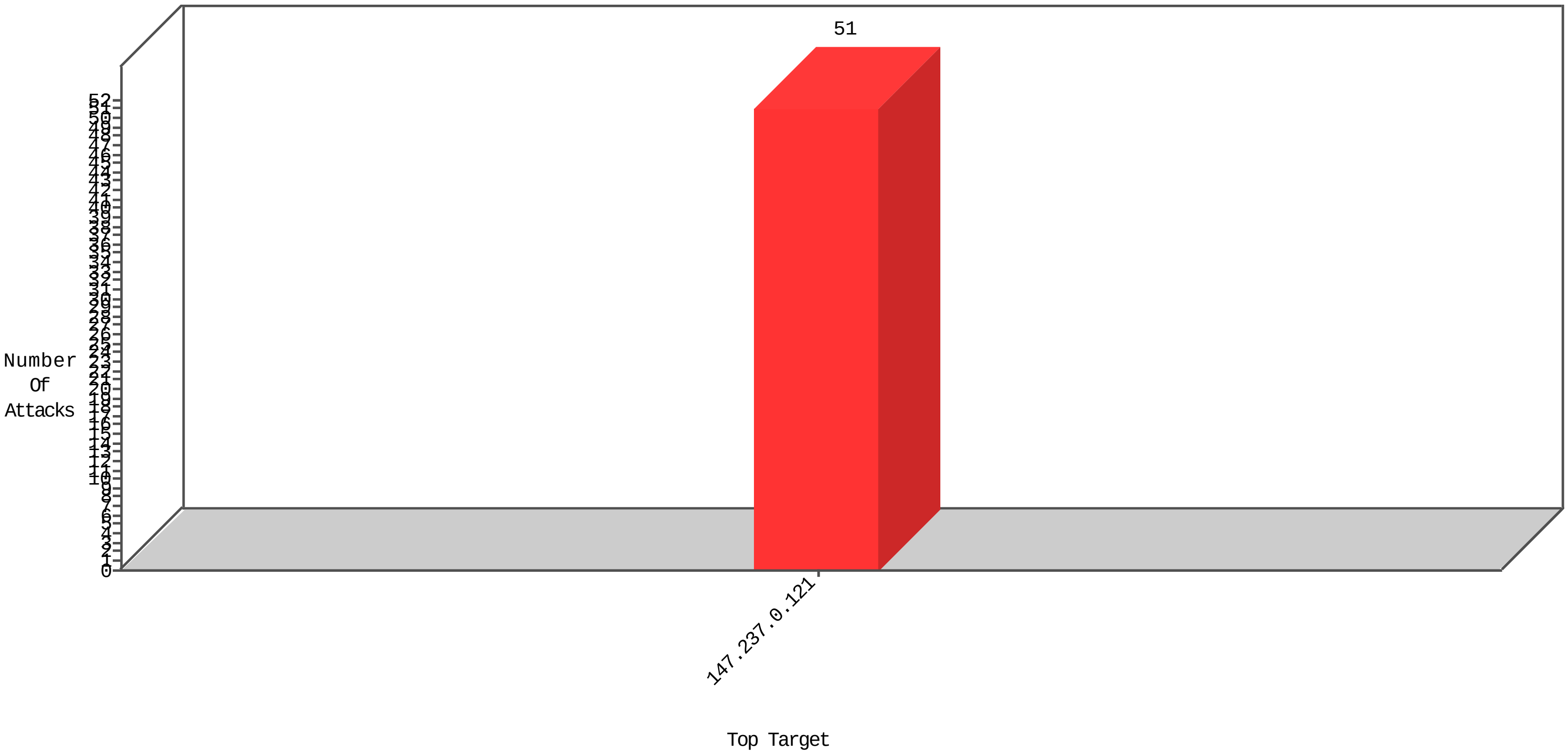
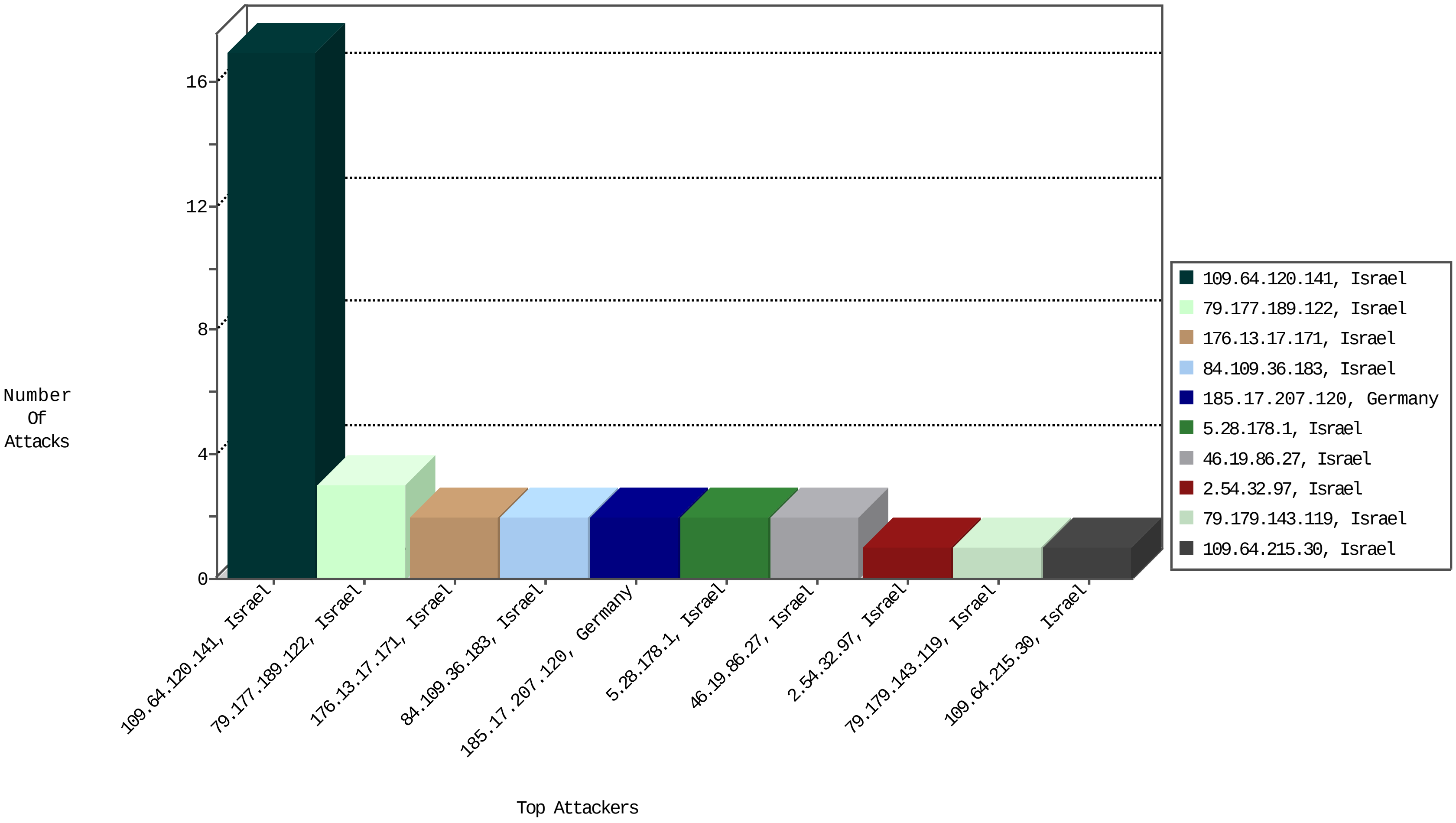
01-16-2016 to 01-17-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-16-2016 to 01-17-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count

01-16-2016 to 01-17-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-16-2016 to 01-17-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
119.164.254.57	China	147.237.0.121		ET SCAN Potential SSH Scan	1

01-16-2016 to 01-17-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
84.109.57.34	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3092
77.125.98.159	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2214
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1236
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1050
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1043
62.168.35.67	Czech Republic	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	297
149.78.229.33	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	205
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	121
149.88.222.111	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	110
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	109
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
149.78.229.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
5.28.175.91	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	54
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
77.125.98.159	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	47
202.91.87.130	India	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.78.225.6	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.74.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
149.88.110.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
157.55.39.174	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
77.125.87.41	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
66.249.81.129	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
183.79.221.191	Japan	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.74.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
84.108.71.176	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	17
94.230.86.130	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	17
66.249.74.81	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
142.4.218.201	Canada	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
54.174.57.68	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.83.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.75.47	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.74.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.83.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.102.7.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.9.22	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.249.74.81	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
184.164.147.18	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
40.77.167.18	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
40.77.167.52	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.64.120.141	Israel	147.237.0.121		Suspicious Response Code	Block	17
5.28.178.1	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected CB7B93F7B4D95FB2019441E58C3D4F12E11F5B38264FEA8735090F6206DC856ADE6046DEF9434B0A4B52C78AB8646B9AF194077985D465A25E96D9F56FD10EB04176AAFEFC19F13D7E0023B87A69FF7B9380E4E48A8F5F5A595F1595CC229CC66A9FF7F9DDAEC00C0EB7AC191C61E30E61874D8A42DDD340E202FE35DC880C66, Observed 62FC4D20FD2966F9754F3FAD4DB2479FE74812691F84610BF84E9A577408DF5EDE76596294123836D8D5EE293FA67BB6FF0EBF7152DF162EA7CF0FCFBA7EDE545EB4FBCC29A0A77ABBC289D583E87FB07F64BE470D1534AC2AC7BD2665218053BCF378	None	2
46.19.86.27	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
176.13.17.171	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
84.109.36.183	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
185.17.207.120	Germany	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
79.182.9.133	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
46.19.85.192	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
152.62.109.205	Europe	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
89.139.55.204	Israel	147.237.0.121		Unknown Parameter na in www.miluim-ishi.aka.idf.il/login	Block	1
79.177.189.122	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.177.189.122 (sigalgs DoS Attack)	None	1
198.20.69.78	United States	147.237.0.121		Unauthorized URL Access to 147.237.0.121/	Block	1
109.64.215.30	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
82.166.247.199	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
2.54.22.252	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
93.173.251.11	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
79.177.189.122	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
31.154.162.101	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
109.253.144.138	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.117.82.69	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
2.54.32.97	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
176.13.17.231	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected E5FBCAD60A9B14583677205996D8037CD24A1EEAB9AEC86A26B55941CECEB40F697BEF9DFC9D5F7D9ABC811B9CE1EFBAAD7DF803EC104F29A0E3B1F467403BF26BC6281C5C8A7B99DF2FF0F938720B0A516F80ADB60B73077A282813A45240319A27278B19B8CF92AE8E0215A9A661D4C4905D5A92D6555B41B5802622C22DC5, Observed 1DB0CD3E58B1593E80C9AE9B39CA09A5D4490AC2381699DEDFA8C254ED0E98A7A1FE780A9DF1AC28015004CC3EBBEB965591146C5309D559A1D19A87E95C116E9FE366711866CF6E16184FA27F99BA768A72723E4163D6DC56276C6E3498821347BC3A	None	1
104.236.46.74		147.237.0.121		SSL Untraceable Connection - Unsupported Cipher	None	1
79.179.143.119	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/l×?×¢×Ÿ×ž	Block	1
37.142.64.16	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
109.253.205.140	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
85.65.103.27	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
79.177.189.122	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value E61559A4146D380303538D9BD83DC7ED79CDE12F5BDB4F439265FD2DDFA9F2C401FC8E3DA41B3A4D117E1BD0799B80298E214BE0E12592F02C9E4731D1CDB887A53088EDAD03F6FBD8D618A7AD0F3C36DC6CB8ABF177D42CAC1324DBA4B4F9A2A8D4F2B69C5CFA49C424FE5ABB5605CDFA19CA576BF32E39720A0965E522CB9801B8042810B9BB61F9674E0281020E1C9036D336133A03F60FE384372D937102	None	1
5.22.135.162	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1