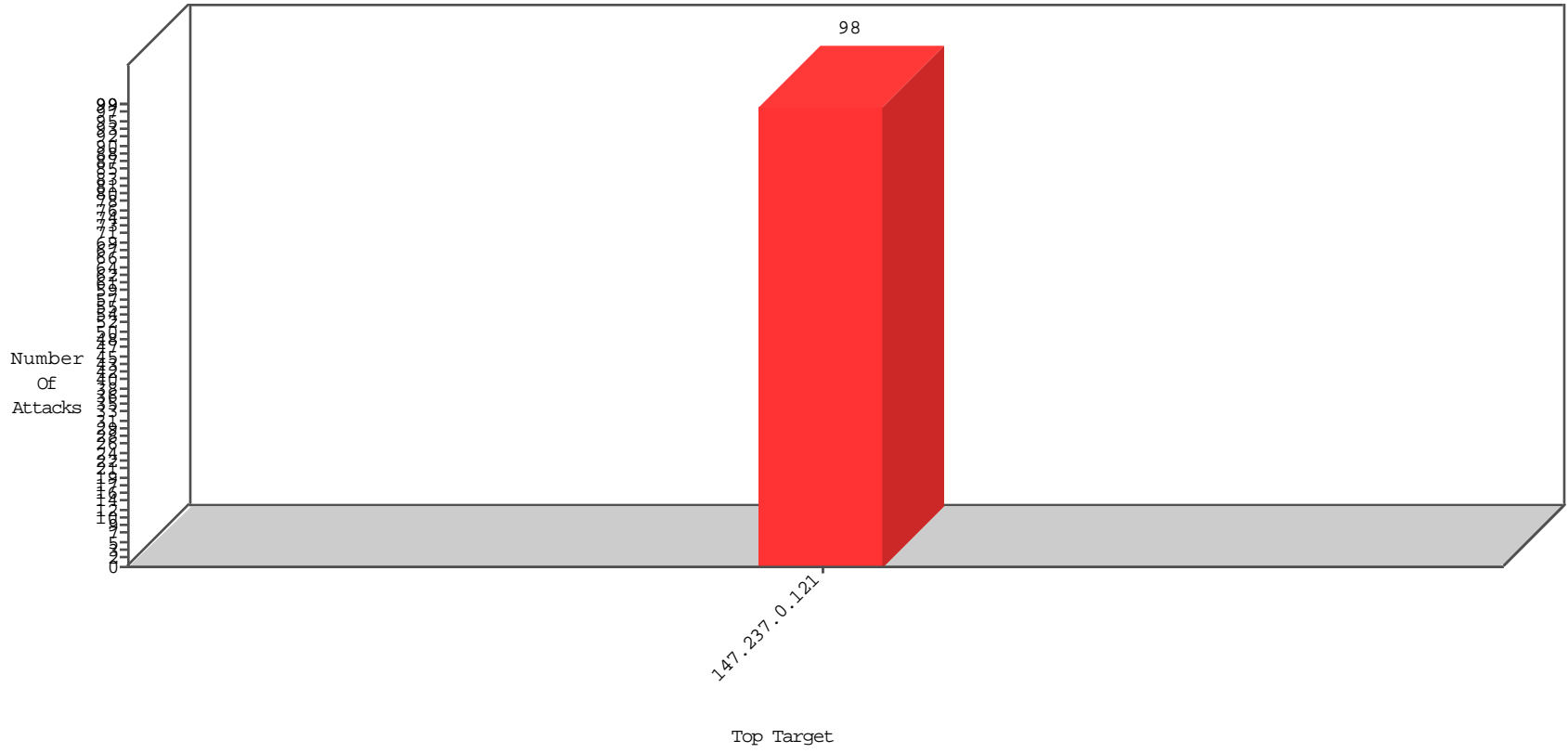


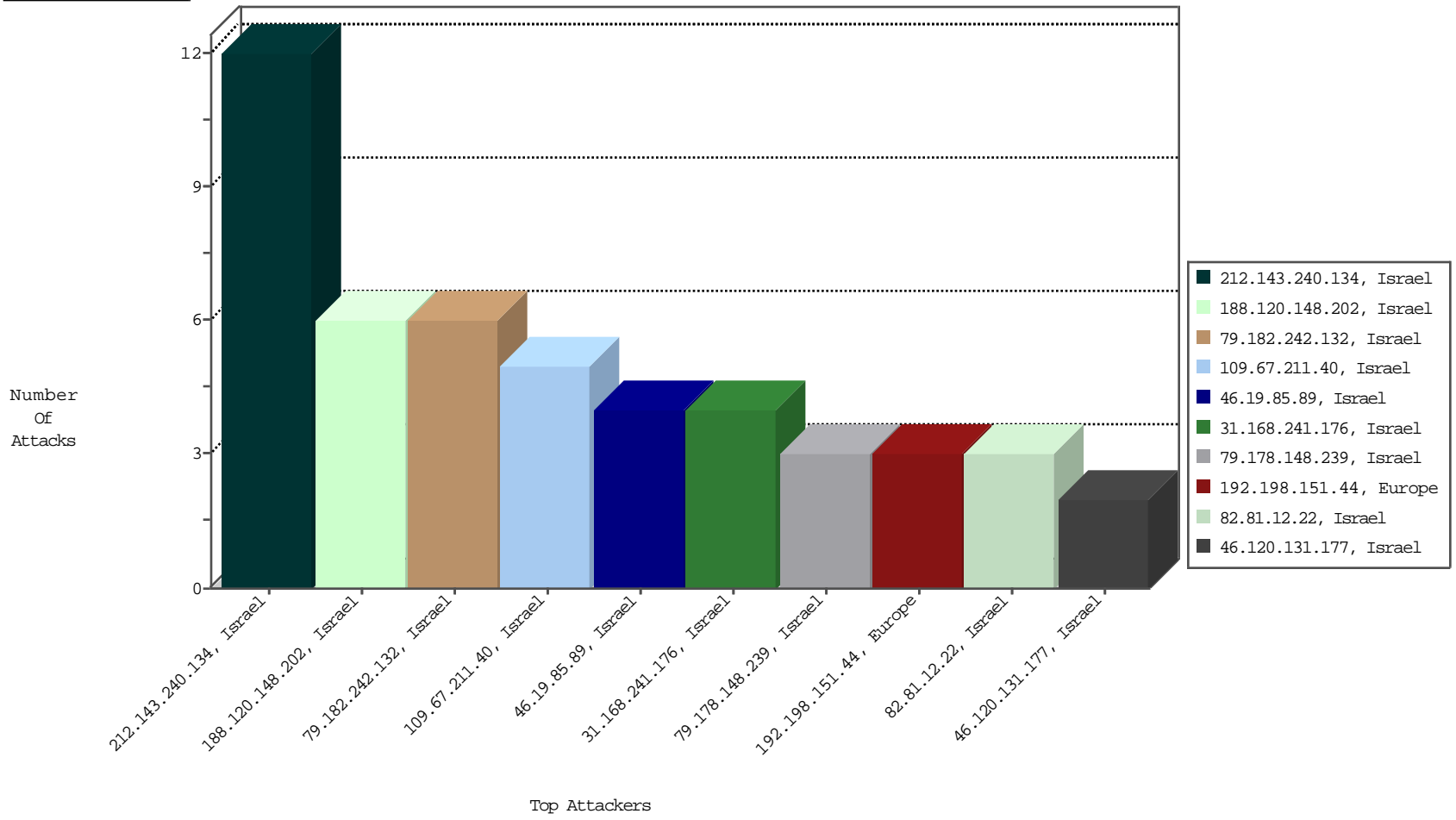
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



02-04-2016 to 02-05-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.81.12.22	Israel	147.237.0.121		Block_Udp_All_Nets	drop	EEL-Isreal	3

02-04-2016 to 02-05-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

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)	2
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	2
91.203.194.156	Russian Federation	147.237.0.121		ET SCAN NMAP -sS window 1024	1
210.217.58.231	Korea, Republic of	147.237.0.121		ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
109.186.5.134	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3032
149.88.109.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	645
79.177.51.158	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	531
149.88.192.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	340
149.88.123.23	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	318
149.88.12.138	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	310
149.78.255.217	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	296
149.88.45.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	285
62.90.235.247	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	243
149.78.46.44	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	240
80.246.139.202	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
134.191.249.39	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	231
176.13.8.179	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
149.78.170.220	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	224
149.88.14.55	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	190
195.52.121.70	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	185
194.90.25.122	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	182
100.33.55.196	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	175
213.61.227.39	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
85.158.139.101	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	169
66.102.6.90	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	163
144.24.20.229	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	156
79.179.96.232	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.12.229	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.200.137	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	140
149.88.230.167	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
149.78.9.128	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
87.237.218.161	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	123
186.155.201.138	Colombia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	118
149.88.206.21	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
149.88.92.210	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	99
149.78.243.115	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	94
161.69.163.25	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
149.78.232.81	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
149.88.140.69	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
149.88.69.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
137.254.4.12	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
149.88.90.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
77.125.145.75	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
149.88.112.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
140.101.20.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
149.78.249.38	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
149.78.227.116	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
40.114.210.53	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
149.78.39.47	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.88.158.152	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
81.180.66.34	Moldova, Republic of	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
149.78.40.38	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.143.240.134	Israel	147.237.0.121		Distributed Unauthorized HTTP Method	Block	8
188.120.148.202	Israel	147.237.0.121		Suspicious Response Code	Block	6
79.182.242.132	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	6
109.67.211.40	Israel	147.237.0.121		Suspicious Response Code	Block	5
212.143.240.134	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
31.168.241.176	Israel	147.237.0.121		Suspicious Response Code	Block	4
192.198.151.44	Europe	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPass in www.miluum-ishi.aka.idf.il/login	Block	3
147.236.232.73	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	2
192.116.53.143	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.178.148.239	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	2
212.179.34.116	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
46.19.85.89	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 1AC485B3E43B3489F22F35719A54CA7164DB64070380211489C6B333995D824D32ACFE50AFF084EA9A8EE6CA91B6D253DAD971D5DD031D6EB2D20442B2EF14C40E785BF1C16EB9A58910E64F045BB17361FE2DF19898BEF623974F5A4AB9582727403E2FA88E541F5AA983167CBC2641607759187826C124662A82D3BC126413, Observed EB8931C09C3383DB67F2DC6B4EC389FC7A291DB570A23A78230303A28B538946B8A21B0281930DDEE0F9F6C0350E1073946683A4C56893188187F1CF73FE32527DDC3E22247CD2258C66A9387C9C809860E9C28ACA977339673C1AC7A7B853AEC8DD4F	None	2
87.69.178.30	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	2
194.90.36.155	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
46.19.85.89	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	2
84.109.116.235	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	2
5.102.203.54	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.110.39	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
79.181.169.40	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 02B70655DABA1F365B2F980A157D0D2CA327EADC35741A6F556B45442AE0553279140616B54B5CB109FA85E8CF7B591A5C3F177052D6D788B919DDCFE161B91556A4539572DF9CF50A6BF8E98A4AF705C7211649A9DEC4AC9CCE02190BBC2EF0997B927AE7BB4C639AAE11834BF4F6AF918993BC8AA3ABD5485084DFD5E3D8C5, Observed 07D96B74EF694D234B8B42A67629C06529F50DBD142F7232FE533D9C840121834B50528B6D76C1EE0F10AD62DB0E06B69447E928380F5B330BCE10903AF0E3EEAECFB3C49A3CA1C7EE5272C5AC7269C8DC010FF3AF65C4ED40BAA244109F792C021307	None	1
79.178.114.135	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
31.210.179.166	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/changeunit parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
95.86.121.179	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
81.218.186.126	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	1
79.179.221.221	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
217.132.36.35	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
194.114.146.227	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
46.120.131.177	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
31.168.193.119	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
185.24.204.41	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
87.68.37.200	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
79.182.66.58	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
2.54.21.170	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 0D1A97EB8133973237878031A362525F745A2CF84B2FC25652518F3736E3C50FC34E64E54FF4A7F7F23143F82AA7C2DF706AF10E4C8C1E46BCFA5DA65230D9EA9A40C1E29A035615573D98E104AC89FBCC88E78A3B7300508335CCC5D1AAEBFA37322E0449D9853FF81677CC0AF3B7805CAE6C728E6297DF0AACF77E477D333B, Observed DB005CA741C55454E445879BDE5D003EE53E9B9AA0B7C482DCA3F9ABC053117FFEDEC93CC0789385D4D6DB1A0EB0A085196D63307842EA43D2B7910B56364D61F915D03D97BB444D2B165DB2CEA71B38BB75916C19C69204D7027767AE2E579B1BBACD	None	1
84.95.211.33	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.180.171.250	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
212.143.154.105	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
46.121.73.221	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
31.168.238.226	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
79.178.148.239	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
212.235.96.66	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 212.235.96.66 (sigalgs DoS Attack)	None	1
2.54.27.178	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100 in www.miluum-ishi.aka.idf.il/fom3010	Block	1
109.253.203.83	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
79.181.132.84	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
79.178.114.135	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
192.115.190.190	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 192.115.190.190 (Open Mode)	None	1
87.69.245.216	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
80.246.137.240	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
79.179.219.56	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
212.235.96.66	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
194.90.199.242	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
46.120.131.177	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1