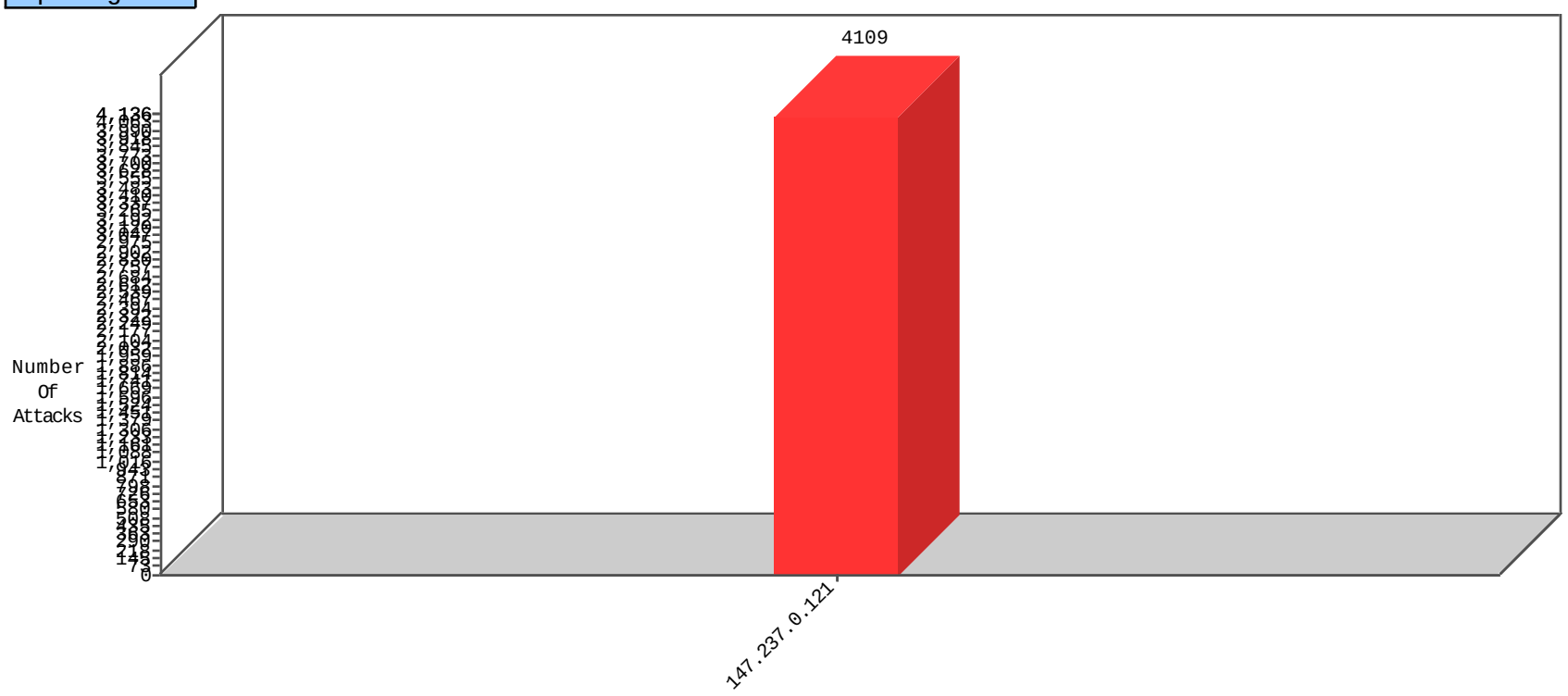
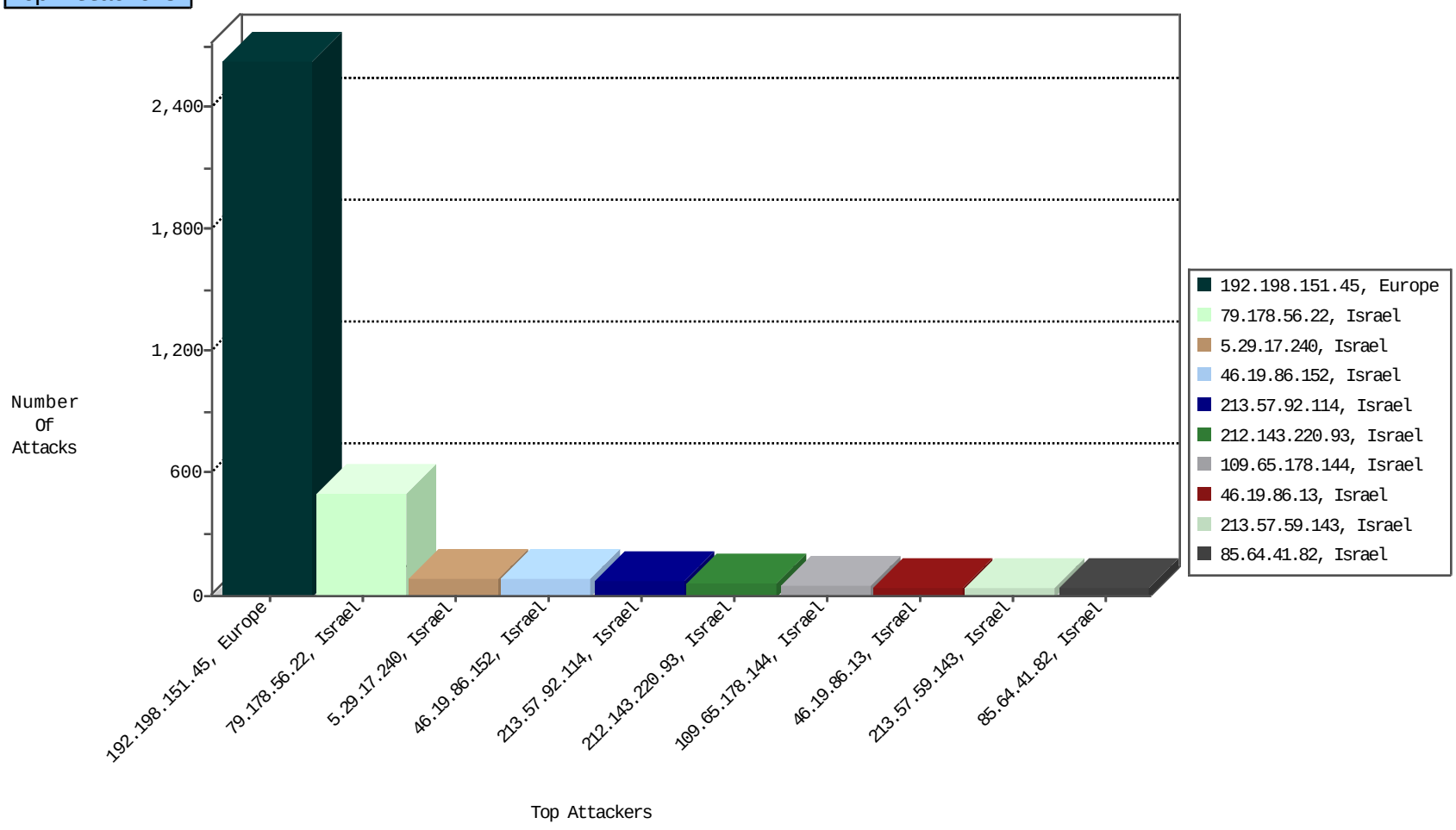
10-20-2015 to 10-21-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



10-20-2015 to 10-21-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
192.198.151.45	Europe	147.237.0.121		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	2632
46.19.86.152	Israel	147.237.0.121		Anomaly-TLS-renegotiation-Cli	dest-reset	BBL-Israel	81
46.19.86.13	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	41
62.219.254.22	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	21
212.25.121.195	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
149.78.195.103	Israel	147.237.0.121		Invalid TCP Flags	drop	BBL-Israel	2

10-20-2015 to 10-21-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

10-20-2015 to 10-21-2015

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
114.38.28.41	Taiwan	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.34.229	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
110.180.44.65	China	147.237.0.121		ET SCAN Potential SSH Scan	1
182.209.172.140	Korea, Republic of	147.237.0.121		ET SCAN Potential SSH Scan	1
212.7.199.208	Netherlands	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1

10-20-2015 to 10-21-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4419
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3792
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3265
46.19.86.25	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1296
134.191.232.71	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1152
149.78.45.230	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1017
149.88.153.123	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	648
149.88.41.26	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	507
192.228.94.56	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	484
169.253.194.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	413
149.78.63.20	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	377
149.78.38.173	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	371
149.88.8.107	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	368
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	364
91.108.183.50	Sweden	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	355
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	346
149.78.249.144	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	338
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	309
149.78.43.245	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	288
78.108.139.193	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	276
149.88.149.123	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	248
149.78.247.7	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	230
149.88.225.156	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	222
111.118.145.241	Cambodia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	210
223.207.117.25	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	200
74.6.254.103	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	183
5.28.180.179	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	178
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
178.162.211.222	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	171
5.157.38.34	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	166
167.220.196.103	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	153
66.249.81.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	151
17.78.99.226	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	146
190.56.171.78	Guatemala	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	142
149.88.37.201	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	139
203.189.137.220	Cambodia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
149.78.68.25	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
76.126.12.5	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	128
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	124
66.249.93.241	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
169.234.226.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
136.237.18.10	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	106
73.219.249.100	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
66.249.93.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	97
149.78.35.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
209.99.2.214	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	91
149.78.196.198	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	88
195.235.52.107	Spain	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
149.78.249.48	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.178.56.22	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	260
79.178.56.22	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	244
5.29.17.240	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/changepassword/newpassword parameter ctl00$ContentPlaceHolder1$txtNewPass1	Block	90
213.57.92.114	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	78
212.143.220.93	Israel	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	52
109.65.178.144	Israel	147.237.0.121		Parameter Type Violation __EVENTVALIDATION in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	52
82.80.143.133	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	39
85.64.41.82	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/changeunit	Block	26
213.57.59.143	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	26
82.80.134.206	Israel	147.237.0.121		Unknown Parameter Returnurl in www.miluim-ishi.aka.idf.il/login	Block	26
79.180.148.141	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	26
80.178.8.133	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/login parameter ReturnUrl	Block	13
213.57.106.36	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	13
46.19.86.213	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/login	Block	13
199.203.11.166	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	13
176.13.13.219	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtVitur in www.miluim-ishi.aka.idf.il/leaveinunit	Block	13
84.228.123.192	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	13
46.19.85.108	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected DECD8BE2A14F6B67235392C73CC3A79057E4522E7804CAFB3E91C232D5DFF557F689059E0FA8A44F787405B802619B7E19406D1D5ABECACBE303D22ABD89EB39CBB2559A6C838F0BF25DA56ECC1CDDFAA132E5B1AD4DAE7DF88EE20C8D46665CEC738E2DC9C808D82986685EBD9374DFE105F3F0519ECC1D097E622DD75B2613, Observed 0408EE0E601248847F1BC665FC897BD6AC60D819596642701CAEBB1EE418939D52A0D453E1AEF236F808856BA7F6CDA162F39EB2B231E68E632125F51DA6A1A1E50C33711595F1A7A8D6E1A3AF997010B604DEDB0D8D91C27080BA5545130986F8F6F0	None	13
213.57.59.143	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 433E70E0C54C20A9E6807C6CA93413BA6C85DCDDF14ED11928FE19C6BABBF50F3A7461A013E5B2305F6CEACDE02C84F27DA1AC11DE86EE7F79D0AC6B3D1FF09A97E167DAAAC52709619877947753C7DF15AB675BFA3D33D888C258E7FBB334EB766AB2F2EF7AA5FBC6B71F1FEC33E5A0C22D6F0191531190683C7D4D6BF91E0C, Observed 2D96AF395074009AACF4C30140447062E88F7AF69B5B89758F8D5A7F4AB21592BB5A3D86760855B3EF431C27CF4CA7116FDF9EED1BE778E13B309BA44D4321FEA5D02A85CBB8706BF2774924D25FD98FC67F2BED4B9A752B0FAF640E44B5586EE923A8	None	13
185.32.179.103	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/login.	Block	13
109.64.145.7	Israel	147.237.0.121		Unknown Parameter tzav in www.miluim-ishi.aka.idf.il/login	Block	13
80.246.137.131	Israel	147.237.0.121		Parameter Type Violation ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	13
62.90.126.74	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	13
5.29.206.162	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	13
185.27.105.106	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	13
46.19.85.223	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.223 (Open Mode)	None	13
192.198.151.43	Europe	147.237.0.121		Unknown Parameter zi in www.miluim-ishi.aka.idf.il/login	Block	13
2.54.11.22	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 5B1054901D6171C9FA63B8005B0FE822A57486DC8B51CD1CE8A837D62663323439F32E3B64882ECA15F6310439312007244A849DCD2D4C8299A18B02EE9B2240A88C3277B5F59BBA3BAE95CC04862B1E26749FED6AB83FE60A0F997C3A1CEC469A5943CF90BD8C5A13DB250CB2820E1F8EFFD9C3AEE42A89D02CCB710043AC794CBFD9ABB28A027139FAC6BBDB9DC7BABA7C6C828590FBCA3B69053DA1D1B580	None	13
62.219.147.213	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	13
31.168.89.107	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesIDs in www.miluim-ishi.aka.idf.il/changeunit	Block	13
212.143.220.93	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	13
185.32.179.3	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 185.32.179.3 (Open Mode)	None	13
85.64.41.82	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	13
46.19.85.223	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	13
199.203.11.166	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	13
2.54.148.40	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	13
109.66.152.124	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	13
79.176.182.251	Israel	147.237.0.121		Parameter Type Violation ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	13
37.142.64.46	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	13
213.57.30.208	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	13
185.32.179.3	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	13
93.173.248.207	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	13