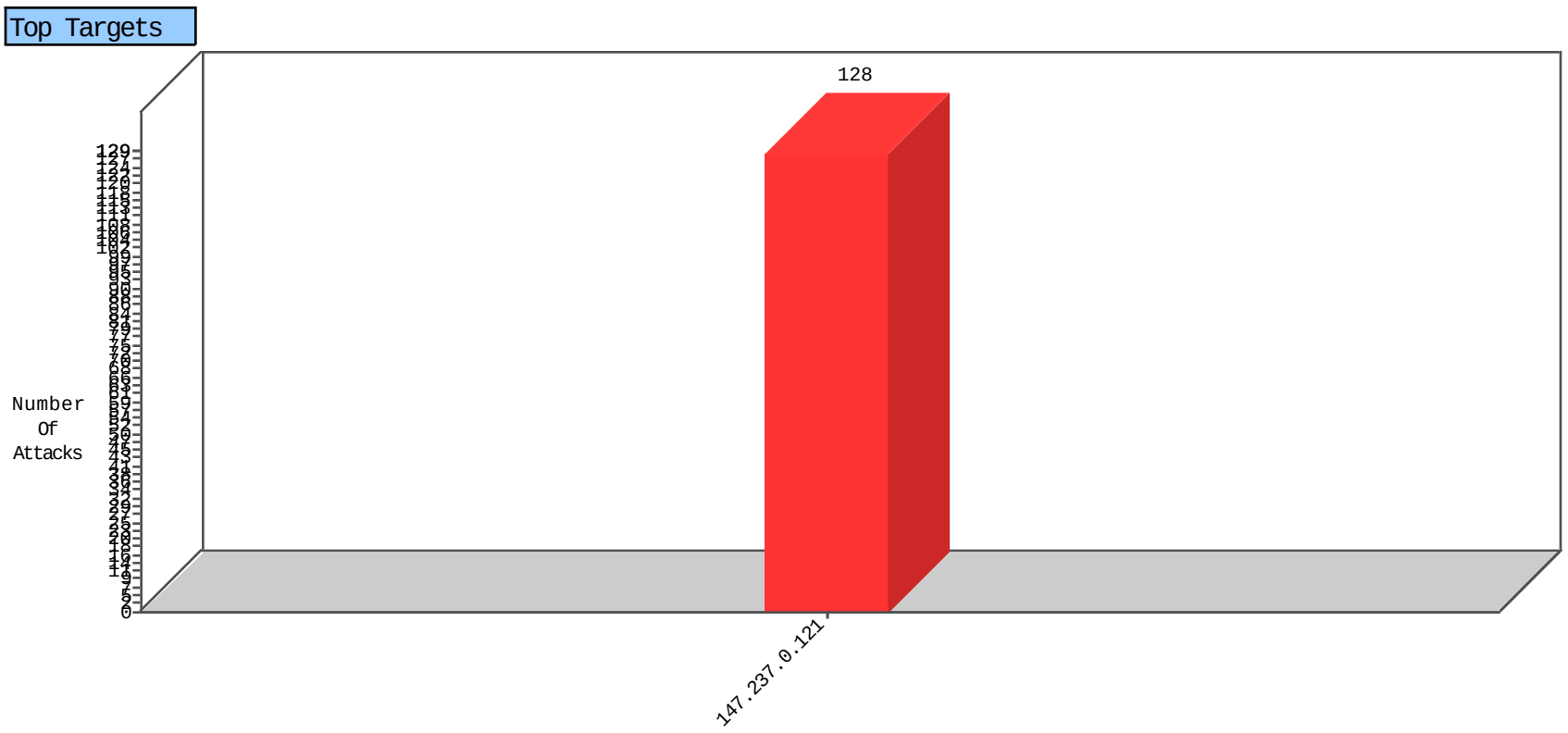
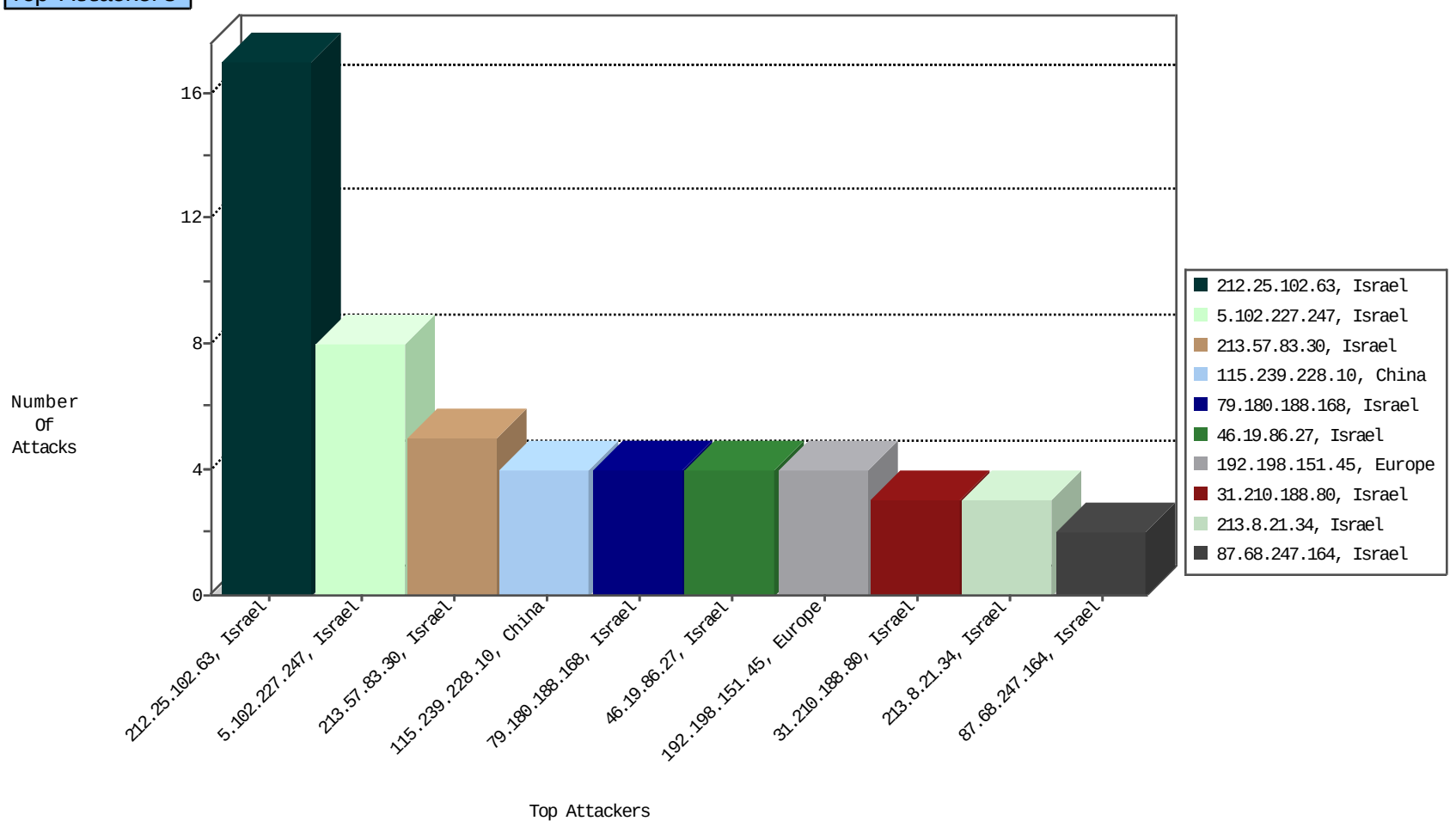
01-18-2016 to 01-19-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-18-2016 to 01-19-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
115.239.228.10	China	147.237.0.121		Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	2
115.239.228.10	China	147.237.0.121		Frk_Under_Attack_Con_Http	drop	BBL-Frankfurt	2

01-18-2016 to 01-19-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-18-2016 to 01-19-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
82.117.208.243		147.237.0.121		ET SCAN NMAP -sS window 1024	1
168.62.238.153	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
199.191.56.187	United States	147.237.0.121		ET SCAN NMAP -sS window 3072	1
113.171.23.126	Vietnam	147.237.0.121		ET SCAN Potential SSH Scan	1
193.105.134.220	Sweden	147.237.0.121		ET SCAN NMAP -sS window 1024	1

01-18-2016 to 01-19-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2217
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1779
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1678
77.127.199.116	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	909
103.246.37.108	Singapore	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	604
149.88.90.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	441
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	416
157.55.39.37	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	299
149.88.20.235	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	290
149.78.146.123	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	194
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	191
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	188
217.171.42.130	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	169
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	160
213.8.204.64	Israel	147.237.0.121		drop	SAM rule	drop	150
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	124
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	121
149.78.225.46	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	115
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
188.180.110.11	Denmark	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
149.78.229.33	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
149.50.77.180	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
84.228.190.194	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	62
157.55.39.225	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
149.88.158.152	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
149.78.224.57	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.88.141.241	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
37.26.147.159	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	50
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
5.102.240.151	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	47
2.54.3.181	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
17.78.96.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
207.46.13.94	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
2.52.135.191	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
31.168.14.74	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
2.52.166.133	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	26
79.178.152.57	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
31.168.14.74	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
58.8.73.30	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
194.177.16.3	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
79.178.152.57	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	alert	25
80.246.139.198	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
79.178.152.57	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
149.88.203.32	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25

01-18-2016 to 01-19-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.25.102.63	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	17
5.102.227.247	Israel	147.237.0.121		Suspicious Response Code	Block	8
213.57.83.30	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	4
31.210.188.80	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	3
213.8.21.34	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	3
80.246.136.95	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
192.198.151.45	Europe	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	2
109.253.141.131	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
82.81.47.19	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
80.246.136.100	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
192.198.151.45	Europe	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	2
46.19.86.27	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
213.57.84.132	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
109.66.49.98	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.64.17	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
193.34.57.101	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	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
84.109.136.102	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
217.194.198.125	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
109.186.13.217	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/templates/personaldetails/	Block	2
84.110.211.102	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
37.26.149.212	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	1
212.143.124.1	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.179.25.200	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
62.219.140.79	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtBName in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
46.19.85.81	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
87.68.247.164	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
37.26.146.155	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.161.241	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
198.20.69.76	United States	147.237.0.121		Unauthorized URL Access to 147.237.0.121/	Block	1
79.180.188.168	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
176.13.2.123	Israel	147.237.0.121		Distributed Parameter Type Violation on miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
77.125.156.36	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.19.86.122	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.64.105.129	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
84.111.160.128	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
37.26.149.219	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	1
31.168.193.96	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
212.199.106.194	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
79.180.188.168	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddAddressAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
109.253.216.200	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	1
77.125.81.123	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
87.68.247.164	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
84.108.82.79	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
37.26.146.203	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
5.29.217.152	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
79.183.53.181	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.176.99.63	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
185.32.179.153	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
46.117.141.221	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
87.68.65.88	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
80.246.137.130	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
79.180.188.168	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
109.253.218.141	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
77.125.147.8	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 77.125.147.8 (sigalgs DoS Attack)	None	1
87.69.165.101	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 247D5FE4AE25221D27B14B4A1B941B411AFEC47922C9EC7D29A6D1D19E58F9D6879F6B5449882C3C3207D5CF9BD75EBC6E613585FEDB480B4A46025A03321C5A87369BA8EFA9FAE10746F98A0DFB251AFA2402E1DF207D62A40D94EC49DABD6A2EBDEC563A943C9202E593E0D4E13F4F6528A2FD8DA2A04201AC4833CA904197, Observed 96545CAE6571FF89FF2412D5B7FFA438DF0C73AC3CEA62B4A77BF9B49C8ACC73BE60A2979C3801939931425125 1825F758F4791A1A00C99B73F0FE61AD8098A4F01A4801666FD21CCE852D903C4812E56B369DCA18A885B2D7C07FFC8A67411CCABE20	None	1
37.26.147.159	Israel	147.237.0.121		Distributed Parameter Type Violation on miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
5.102.220.250	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
212.117.136.8	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.183.180.109	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
79.179.25.200	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.179.25.200 (sigalgs DoS Attack)	None	1
185.120.125.39		147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1

01-18-2016 to 01-19-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.210.131.110	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.19.85.81	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.81 (sigalgs DoS Attack)	None	1
87.68.65.88	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
82.80.19.242	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
37.26.146.155	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 37.26.146.155 (sigalgs DoS Attack)	None	1
213.57.83.30	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected C927F45DCBF4E797AA7CD981E3E5C7506627D4EA40F3111313F18026FF8961F35EA55C48253F6B92F18A4F6492CF002D325626A1DDBE9D551E9A1187594EE68CDAA9895E7D83BFDAB327515A03207FE56F1ABDC4142D021CB27625C19CB50B8891A573B5E51B579467FDB207D673CE9F76D34E7E6A2B8CE12A795309AB010BA0, Observed 184DFB9A2188DF1B9618A089230768AD55BCFADD8C9F06CFB9C5C904D339858BDB9153C658FFECCD9FDC84541398567543BD6C16D30E20DFB14BCE812D2FD27E826466B47312E5D9DED2E715FCD668212C242D89F352B1E198454B0747E250290BDBED	None	1
79.180.188.168	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
194.90.99.129	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
132.70.66.13	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 61F6325E56FB354C0705498B7A4B774C52331DEB1EA053645BE99E429628ED0AA2140AAEB1857CCB42FA58FE63F25D5E69FCE7EA4032A907D4BA72BAFB998E369ABEE4EAE137A3C7E56EF82C2FC73AC1515FC40163BAB2CC11481B860586CE56026AE215F2A8D460D2790A36B53EBB7552C4C1352C25DD78C30D85F9CD2F835E, Observed 50D6D64621122560C63EA44878861A0874071ACFE4704D788C10397099865E0D55B34B0F90F8ADDABB8FAE9B9F65BAB4B5301844E218ABCD6BFE9A612E47C89736F5A9742F02288B6F68C4C79F155504384FB793C11CDADBDEA30E873AD6D43266C583	None	1
77.125.147.8	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.115	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.165.101	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1

01-18-2016 to 01-19-2016