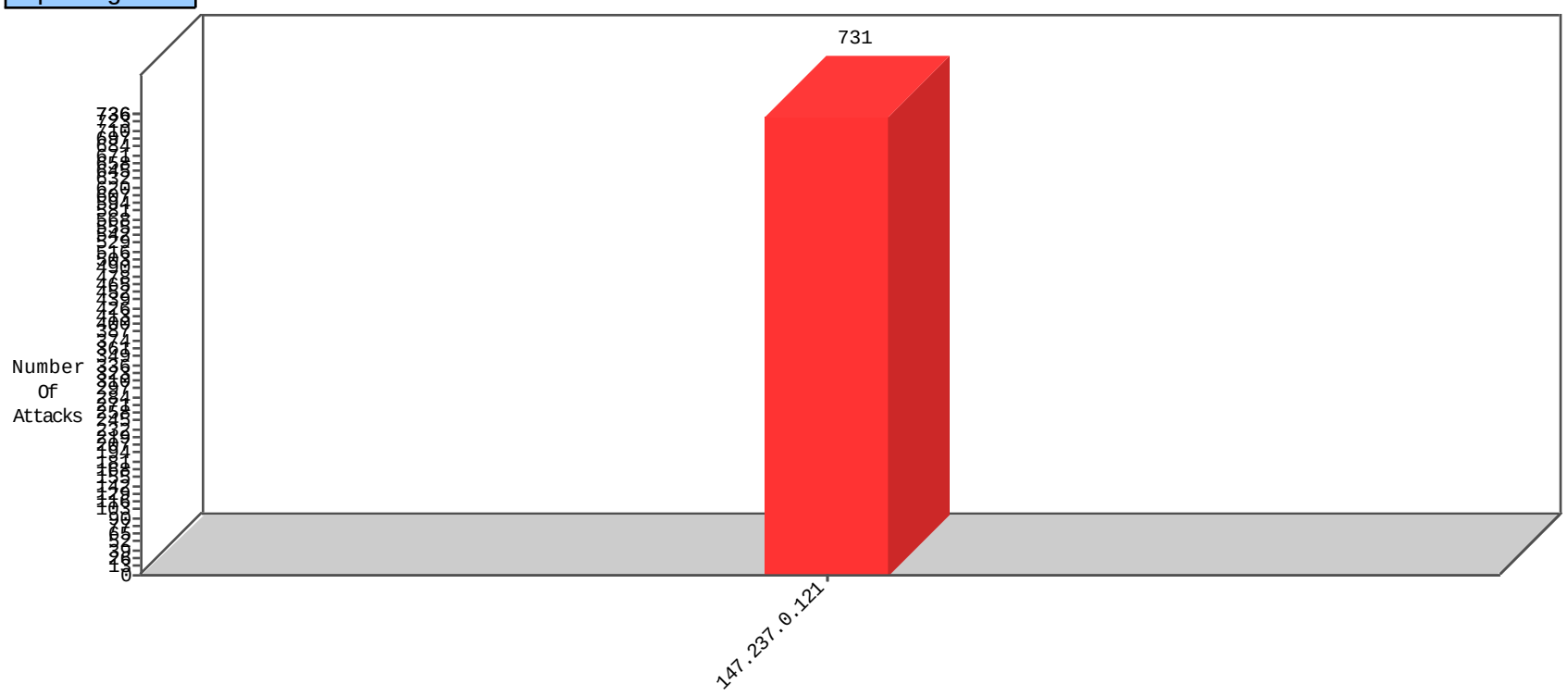
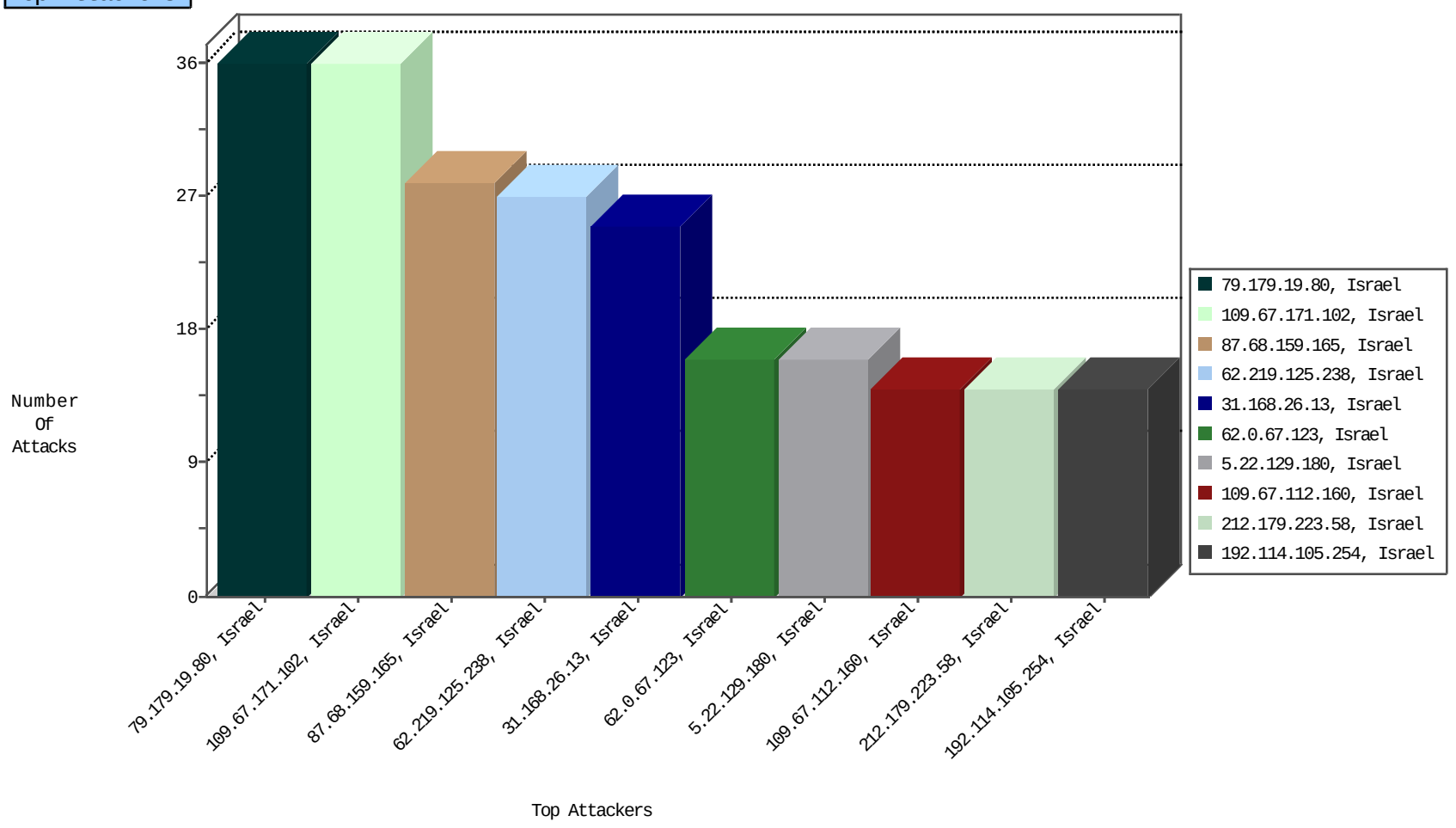
01-11-2016 to 01-12-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-11-2016 to 01-12-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
109.67.171.102	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	36
87.68.159.165	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	28
46.19.85.49	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	5
84.229.243.98	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	5
79.180.39.239	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
82.81.12.22	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

01-11-2016 to 01-12-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-11-2016 to 01-12-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	2
40.122.205.137	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
68.15.122.196	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
109.235.254.181	Turkey	147.237.0.121		ET SCAN NMAP -sS window 4096	1
109.253.138.168	Israel	147.237.0.121		INDICATOR-SCAN myscan	1
218.57.11.7	China	147.237.0.121		ET SCAN Potential SSH Scan	1
223.4.174.30	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
109.253.138.168	Israel	147.237.0.121		GPL SCAN myscan	1
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
222.186.34.94	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1

01-11-2016 to 01-12-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3698
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2301
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2130
158.58.172.238	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1600
109.67.171.102	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	423
12.110.209.245	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	348
149.78.226.247	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	330
149.78.95.197	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	303
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	297
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	295
84.108.101.225	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	260
84.108.101.225	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	256
149.88.105.88	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	249
167.220.196.166	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	249
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	237
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	176
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	165
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	155
149.78.234.208	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	146
94.159.166.59	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.88.186.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	140
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
66.249.83.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	117
195.50.183.212	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
149.78.241.3	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	106
37.227.75.200	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	99
82.166.53.161	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	98
85.18.108.228	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
46.19.86.193	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
62.219.115.209	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
207.46.13.14	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
149.78.231.74	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
192.115.177.202	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	61
149.78.47.118	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
149.78.41.120	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
66.249.69.175	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
149.88.58.39	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
94.230.86.192	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
2.52.48.168	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.49	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.86.46	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.167	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
94.230.86.192	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
37.26.147.198	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
84.229.243.98	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
149.88.183.37	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
194.42.67.50	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34

01-11-2016 to 01-12-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.179.19.80	Israel	147.237.0.121		Suspicious Response Code	Block	15
82.166.58.100	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/$$$&?&?$$$	Block	9
192.116.232.69	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/$$$&?&?$$$	Block	9
5.29.141.154	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
84.108.101.225	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.108.101.225 (sigalgs DoS Attack)	None	3
192.118.30.102	Israel	147.237.0.121		Unknown Parameter **** in www.miluim-ishi.aka.idf.il/login	Block	3
212.199.177.67	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00$txtNewPass1 in www.miluim-ishi.aka.idf.il/personalsettings	Block	3
199.203.211.196	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	3
37.142.237.68	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
2.54.186.164	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.35.185	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
84.109.48.238	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
77.125.106.246	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
80.179.141.237	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.6.255	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	2
93.173.225.160	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 93.173.225.160 (sigalgs DoS Attack)	None	2
80.246.136.152	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
84.109.105.15	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
81.218.145.94	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
147.235.8.37	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.137.10	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
62.219.99.154	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
87.69.4.210	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
212.150.79.186	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
84.109.224.230	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.109.224.230 (Unknown SSL Session)	None	1
192.114.91.249	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
132.70.66.14	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
46.19.86.100	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 00D30DA397BF43D3A5718F5DF4B92A17FEB7EA243406C1A5C7C934C6E26C275A4C6672E7A52FBD66986BBAC049FB49213330847C997F62CEF11BE17546E3853D663DAB14B615002AA746E2A3D93DD37088E48826A82A389B35CF460897A1C686EEC418971A61CCB9DBC1D49E364A130D08627977C3DB0C97F1C2E76A319B1577, Observed 1BD91A07283B3EDE29E117505243533AA166E7A89441EB15C9EDF681526D7E69462D4962948BC29F69CA639ADA371DD2DA76817482A4AEEC3C906E5A4E26D051A1EBFE4C195075FE15743AB1A9DDCFEE612F54E25E5ABE0C04615C0B5EE4DE89E45E1B	None	1
95.86.66.123	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
85.64.181.146	Israel	147.237.0.121		Double URL Encoding - parameter: ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
37.26.146.233	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
213.57.41.186	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.40.230	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
212.29.203.226	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
176.13.6.205	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
80.246.139.88	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 80.246.139.88 (sigalgs DoS Attack)	None	1
109.186.88.234	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
87.69.140.47	Israel	147.237.0.121		Suspicious Response Code	Block	1
46.19.85.138	Israel	147.237.0.121		Parameter Type Violation isCharig in www.miluim-ishi.aka.idf.il/login	Block	1
5.28.140.85	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
212.150.128.10	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
84.109.224.230	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
84.94.107.42	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
132.72.10.245	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 132.72.10.245 (Unknown SSL Session)	None	1
62.90.94.38	Israel	147.237.0.121		SSL Untraceable Connection - Unsupported Cipher	None	1
109.64.28.68	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
85.64.190.120	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
37.26.149.208	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 37.26.149.208 (sigalgs DoS Attack)	None	1
213.151.36.128	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
2.52.47.228	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.68.157.162	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
84.109.105.15	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 246D29F9F0A5D326B5D0420A54EFB8AA9B7385AEAC7E72DC994DB3F00A7166129BAB33BF91561FF691A1E58EB24E7E2D5407854A4ED5D69747C650A817280349877515E8222B91C96D58045B21605275B5F574257FB5572A46A7F84519ED6BFD96C575B0DA40223421D675E2254CAEB7A2FA5520DC450B23B40289A6804F58059E37081520EDE1680EBB3D6CB09A7F6C06F18D38B851DA7EAC88767DC9990B04	None	1
80.246.139.88	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1

01-11-2016 to 01-12-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.253.139.56	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 76D71FC35DD7FA20CF30ED9D4CDFADE810ADA01FEF95C50497EA1CD967BBF5B8089C62BBE488004DA7F866D274624AF1FB6EF53AE77B99E284B29A3549487293009AEEFB2C745159213717B22D55A1FD969F8869E25A5272D828FD3DA71B8E502E16BEB5AA424D1BD934F9D0815E0AB32C3EF243D3D479B93C3806578AA3D9A3, Observed 08DAA77A037EB22399C79C66321A59C2383CD39524827D215271D66D91437F027819868125B8393F9B82637BFB7AF865D49553FE50ABEB5E042107A05BCC3447C869EE5D64D69EF5E753AA5CE7023A78745D1E231CB23E455AB1104A804F56A3AC9421	None	1
79.177.39.84	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
46.19.85.221	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.150.128.10	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	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
132.72.10.245	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
62.128.41.130	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
109.64.185.223	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
85.65.55.8	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
37.26.149.208	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.155.108	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
212.76.97.127	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
192.114.5.10	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.253.223.120	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
46.19.86.52	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
93.173.225.160	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.229.243.98	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	1
31.168.3.154	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
84.108.101.225	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.186.88.234	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddAddressAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1

01-11-2016 to 01-12-2016