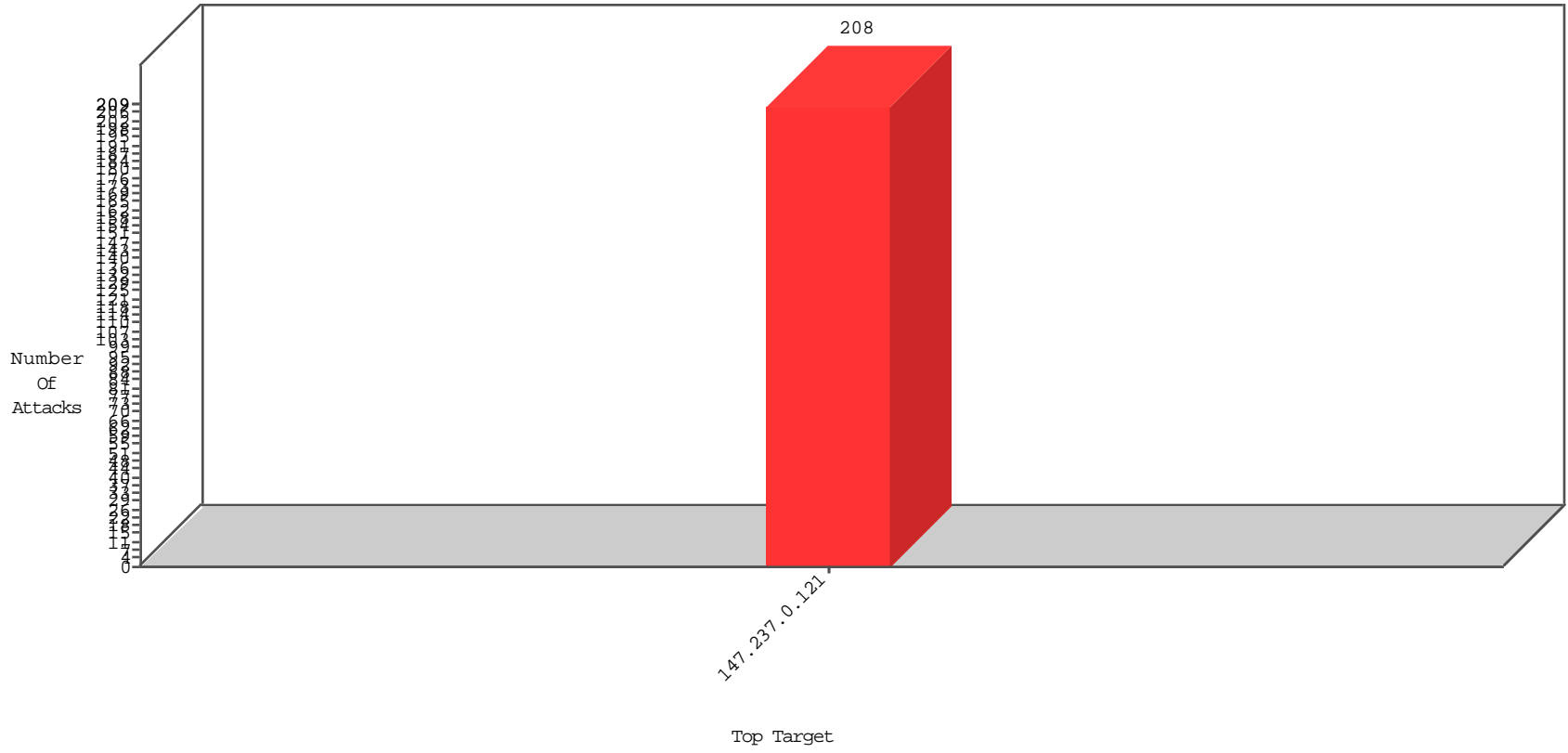


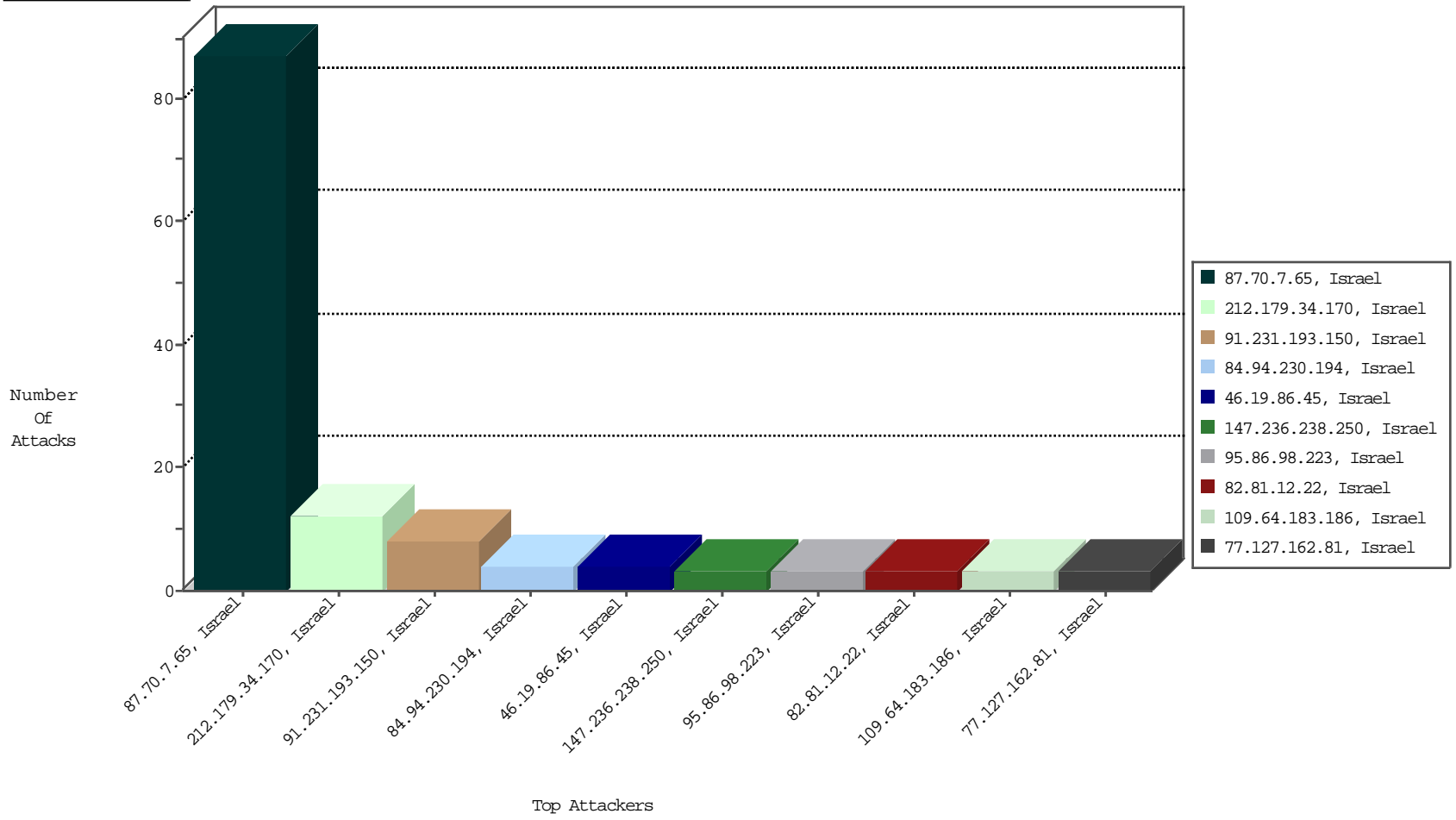
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
87.70.7.65	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BEL-Israel	87
31.168.133.226	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	3
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	3
82.81.12.22	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	3
147.236.238.250	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	3

02-08-2016 to 02-09-2016

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
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
193.201.227.52	Ukraine	147.237.0.121		ET SCAN Potential SSH Scan	1
192.198.151.44	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
149.78.196.220	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1814
17.78.104.113	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1214
149.88.146.176	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	612
194.9.253.238	United Kingdom	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	554
168.87.3.33	Europe	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	433
149.78.81.89	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	397
149.78.169.83	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	393
149.78.34.82	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	311
208.101.23.234	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	300
109.253.201.245	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
199.207.253.96	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	288
165.225.72.54	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	287
149.78.231.161	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	286
149.88.103.190	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	284
85.115.52.201	United Kingdom	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	269
149.78.39.35	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	244
149.78.20.188	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	231
149.78.248.162	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	209
134.191.232.92	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	207
149.78.254.209	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	205
66.102.9.74	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	203
2.54.186.147	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
149.78.232.27	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	174
149.78.32.210	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	171
149.88.54.170	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	165
149.78.210.165	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	153
80.246.136.164	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
80.246.138.21	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
80.246.137.100	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
98.196.39.86	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	142
14.203.110.227	Australia	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	134
149.88.154.143	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	134
149.50.77.180	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	132
149.78.194.198	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	130
96.52.151.38	Canada	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	124
149.78.62.113	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	123
176.98.73.73	Ukraine	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	121
87.70.7.65	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
64.121.88.54	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	116
149.78.11.143	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	114
149.50.101.82	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	112
2.52.48.224	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
192.115.177.203	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	106
192.54.144.229	France	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	104
149.78.40.182	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	101
66.102.9.97	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	101
149.88.90.189	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	97
149.88.31.197	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	97
192.88.162.1	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	96
208.65.73.39	Canada	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	96

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.34.170	Israel	147.237.0.121		Suspicious Response Code	Block	12
46.19.86.45	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	4
84.94.230.194	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	3
109.64.183.186	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	3
91.231.193.150	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.127.162.81	Israel	147.237.0.121		Multiple Unauthorized URL Access from 77.127.162.81	Block	2
109.65.136.102	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	2
192.115.248.2	Israel	147.237.0.121		Unauthorized HTTP Method	Block	2
109.64.147.46	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPass in www.miluum-ishi.aka.idf.il/login	Block	2
91.231.193.150	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	2
2.54.159.58	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.21.194	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
46.19.86.59	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.83.198	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.174.183	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.110.7.165	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
95.86.98.223	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	2
91.231.193.150	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 91.231.193.150 (Unknown SSL Session)	None	2
5.144.62.135	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
79.178.28.198	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.172	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.111.136.54	Israel	147.237.0.121		Suspicious Response Code	Block	1
2.54.191.222	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.179.71.70	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
79.183.102.47	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
2.52.13.250	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluum-ishi.aka.idf.il/changepassword/newpassword	Block	1
185.32.179.143	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.160.168.67	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
46.19.86.255	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.236.18.202		147.237.0.121		Unauthorized URL Access to 147.237.0.121/	Block	1
91.231.193.150	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 91.231.193.150 (sigalgs DoS Attack)	None	1
31.210.179.166	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	1
2.54.152.135	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.76.97.211	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
79.179.98.170	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
176.13.0.26	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected DC82148B8FBE895F61750F96D0200BAA8A78A9F9A335EC54F8B580FF20E1D00328FAE92AF429 93A01CE0CA1283F3FD65B1834362BA9A4C952B363768FB2E6B7271FBEBC8D044ADE080B22 4D265F629C67769F0B6C5CCC9DDB2639CC72FA2C3A6EA757A47ABB803C6D5A0A89AD961D 476B3AA69A7A23E9F569D03D404B3FBFC, Observed CA2D06269AC4D5E29DD27B152E326A3550C054E891387731D83AA592E6D9D74DCA3CC476B 9B9802649F64EF0199400F06841AA79C0952F29E257547500E19C314588FC2176D9B2076A124 AEE7EFF07F65671619BB620B0D5B1DE804C42F7171CA68E17	None	1
62.219.236.36	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
95.86.97.26	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
85.64.177.242	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
5.29.53.251	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluum-ishi.aka.idf.il/changepassword/newpassword	Block	1
80.246.136.56	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.17.58	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/newpassword/firstlogin	Block	1
109.160.168.67	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
77.127.162.81	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/newpassword/	Block	1
46.116.26.25	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.26.146.154	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
84.94.230.194	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
79.180.234.29	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
176.13.1.146	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.113.43	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected A5E8BD8EE634E31AB79579F99314B74A5F626156CF897355429D59255E6AE6CE01F3B64241226 302FA5B178CBF12132803E030BC56F5F7B1DC9D7B2183F5AA7836C0FCD78D500FF2445EA83EA 79D312783EE94E71F5CA27AF1EAF23C0C1D0CAAADD9C979CDAB42B67731E85D32FD435F261 354D69EFC8A169338CAB665E69E2, Observed 5C03ED1D98C9F5B5C855720916DA645A42CF97372528BEAA198B4A63ECBB6FCAB48B1752DD A24FDD85470C6A51BEE9E252355A41566C154E9671F67180BE1835E14E8D8E0DC3CFAE939C2 3DB1578C274C9F65AEB782DCDAAB14113A0AD52752560022	None	1
77.125.1.125	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluum-ishi.aka.idf.il/login	Block	1
95.86.98.223	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
87.69.82.100	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected C6BE085890C8CC8DC01FC4AC14A239CB87CF77E6671C735EE005AAA6F947EE6E802FDF9F61 9210322B35E0C5233F7489734414AB1E1AD1007937A403EFFE95DEFA872CAF03196812862C08 73733FE84884FDC09C0D6774B46DB46DA171A5BBC991F00F236280601A8CD482C9C170C4DF A1D731DF1419A14C7C4A2881D5C7F14, Observed 957D4784F72B762DD313B5357C2F06883172FF1CB929B31DC295FF9FFFE4159B4A473D391423 384BF8F34B463149CB600C8F9A732D07B76897D0064A4D9E74711847301D9BD298878B57465 3ECDDF784BA837C09B3D957E312F7A883A14EA4DE6DCBBB	None	1
2.52.48.227	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
193.17.42.129	Israel	147.237.0.121		Unauthorized HTTP Method	Block	1

02-08-2016 to 02-09-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.218.83.34	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.176.161.82	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
132.72.10.245	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
62.219.120.114	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
91.231.193.150	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.26.148.195	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
79.182.194.160	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
185.32.179.143	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 185.32.179.143 (sigalgs DoS Attack)	None	1
109.160.168.67	Israel	147.237.0.121		Parameter Type Violation ct100_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
77.125.1.125	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.19.86.120	Israel	147.237.0.121		Distributed Double URL Encoding	Block	1
2.54.129.77	Israel	147.237.0.121		Double URL Encoding - parameter: returnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
194.114.146.227	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1432-he/miluim.aspx	Block	1
82.102.169.113	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
132.77.42.233	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
109.64.185.139	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
62.219.236.36	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value 01CBEDBB5E632FBA10C4298EA597B0FF507DCEA1C6A6ADCD1BD5CB6150C54D77D88D7E2C3CFDDBFEBF111ABC517A7388FDE8D2A90851FB2EB85EFF3AD1845C0F218E2775D8D17175AC111E0C62E2F69464A7D75B2AB369341E0821606265BD92A41983575EF813C47058A032F1C6930B214765A117B810BBF728EF5C1EF4D65699C5E669B2B0A88792D791333B7344F6F085E18B0EF336C930FFAE80578D2082	None	1

02-08-2016 to 02-09-2016