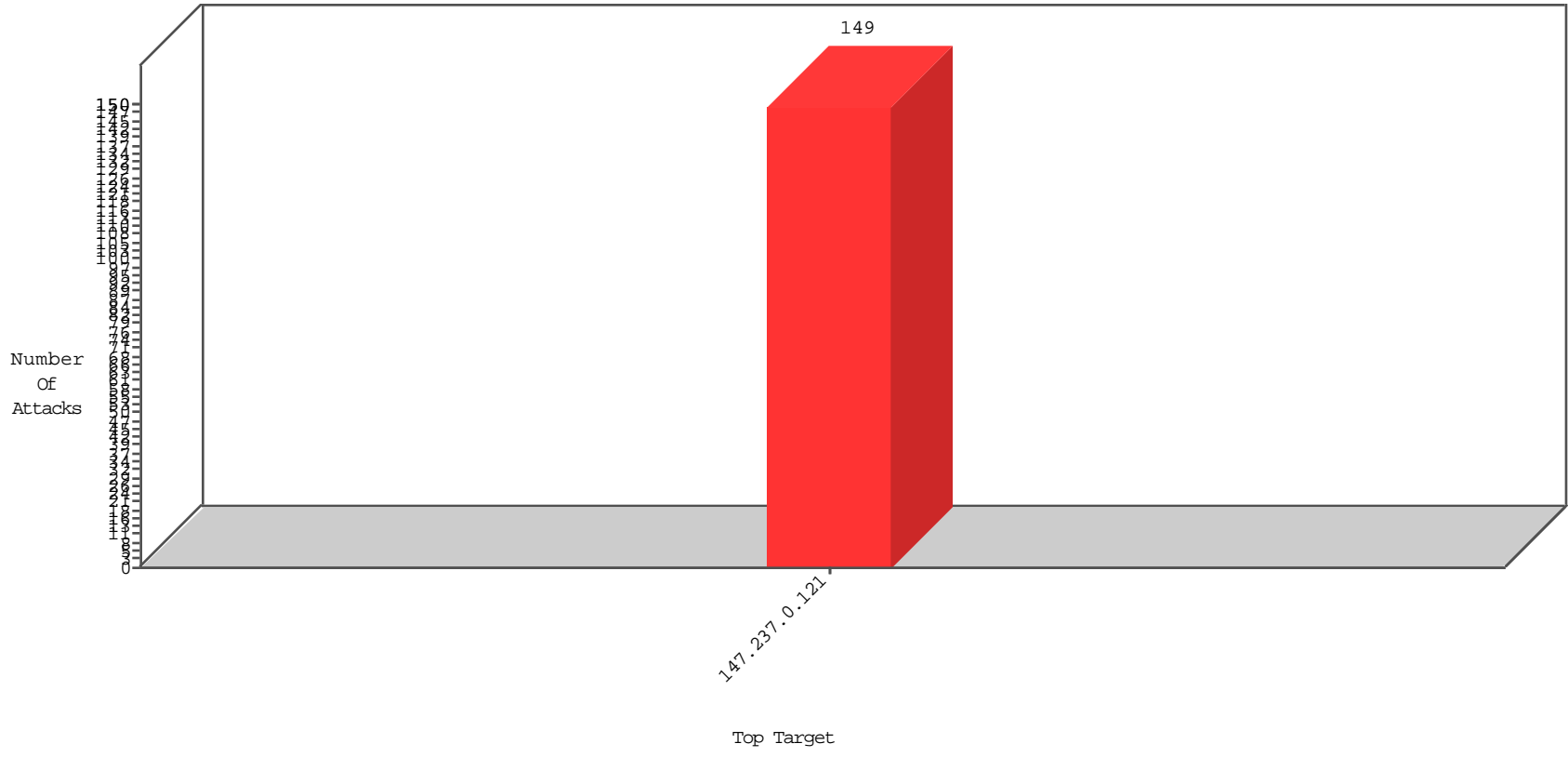


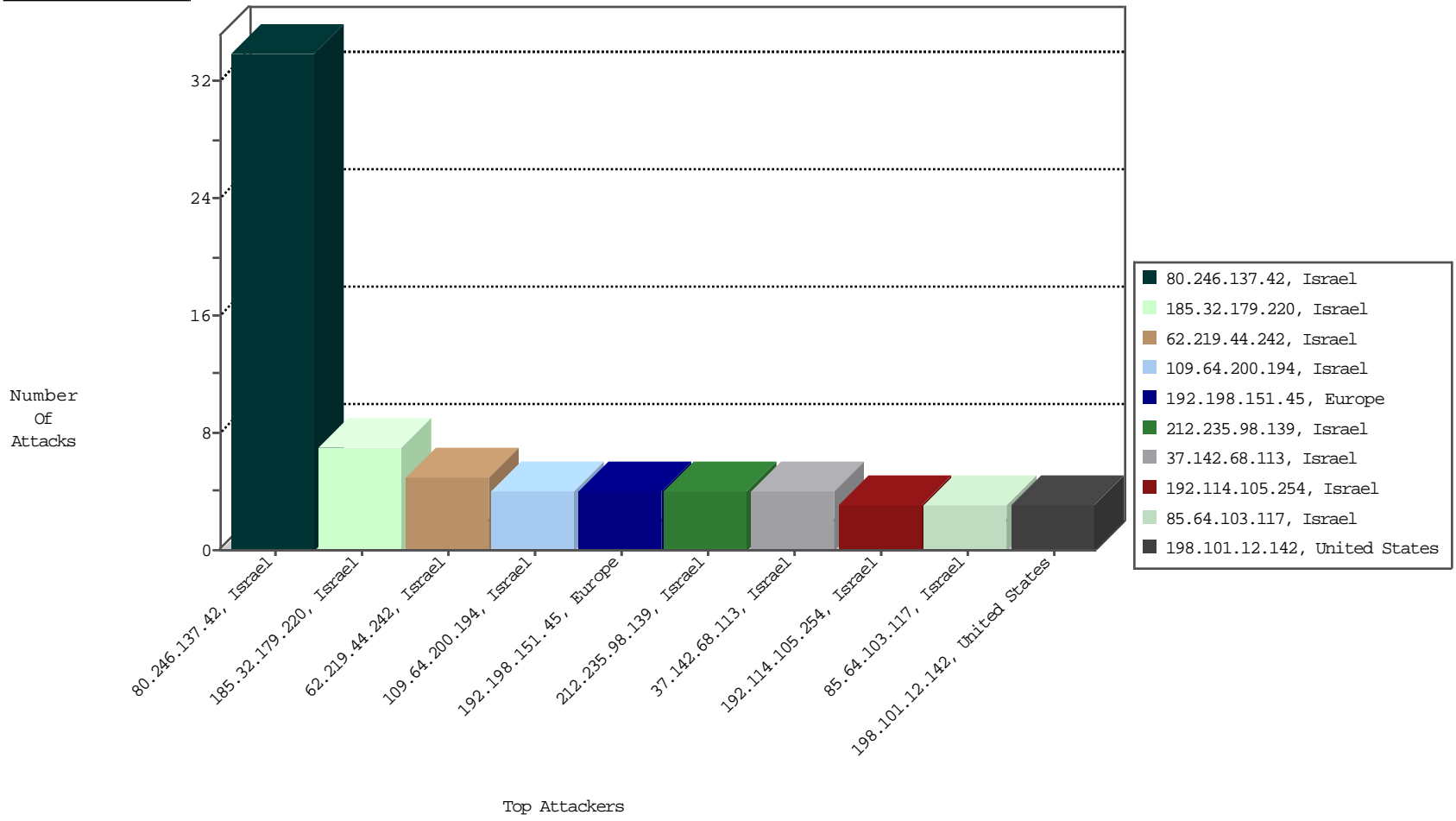
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
80.246.137.42	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	32
185.32.179.220	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	7

02-03-2016 to 02-04-2016

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
123.201.255.106	India	147.237.0.121		ET SCAN Potential SSH Scan	3
188.120.135.12	Israel	147.237.0.121		GPL SCAN nmap TCP	2
192.198.151.43	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
212.66.53.125	Ukraine	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	Netherlands	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	Canada	147.237.0.121		ET SCAN NMAP -sS window 2048	1
198.101.12.142	United States	147.237.0.121		ET SCAN NMAP -f -sS	1
198.101.12.142	United States	147.237.0.121		ET SCAN NMAP -sS window 3072	1
218.1.31.135	China	147.237.0.121		ET SCAN Potential SSH Scan	1
104.128.144.131	Canada	147.237.0.121		ET SCAN NMAP -f -sS	1
115.236.75.201	China	147.237.0.121		ET SCAN Potential SSH Scan	1
162.222.185.165	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
198.101.12.142	United States	147.237.0.121		ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
144.24.20.232	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	757
149.78.237.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	738
149.78.32.224	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	661
87.237.218.161	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	586
149.88.15.72	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	495
194.9.253.238	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	409
149.78.196.32	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	353
149.78.247.98	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	349
149.78.39.47	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	307
149.78.59.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	301
192.88.162.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	298
149.88.78.44	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	279
134.191.232.68	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	277
134.191.232.69	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	248
149.78.255.17	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	226
149.88.45.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	216
149.78.34.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	211
149.78.251.37	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	208
149.88.12.212	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	201
217.194.159.14	Satellite Provider	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	195
140.101.20.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	167
194.90.25.122	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	166
149.88.41.147	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	159
69.158.18.69	Canada	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	158
149.78.241.105	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	144
149.88.154.230	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
149.88.116.67	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
149.88.139.207	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	135
149.78.47.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	131
149.78.139.79	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	123
107.206.249.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	118
109.233.47.10	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	118
50.204.67.242	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	115
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	110
40.114.210.53	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	105
213.93.183.129	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
149.78.235.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	98
149.78.21.110	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	98
149.78.144.57	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	95
80.246.137.42	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
2.54.12.229	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
149.88.70.187	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
149.78.14.206	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	75
137.254.4.9	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	72
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
149.88.194.79	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
167.220.196.115	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	69
88.128.80.132	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
149.78.192.193	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
62.168.56.1	Czech Republic	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.198.151.45	Europe	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 2E1E1E4EE7263E1FBE0E442DB7A66EA9A7B86EA4073FC090CF3C3D474B752498A8F143ED416F0 D2667A4C80D1946CE49165CFD985F3B6C8D3387786829BBC2DECD7E813263DF6209B89715A AD3C25F126C54B85505BF49CE1F1868FC97AC447506C55C68D71F46E49D192800D9AB52617E E0BED981CBF5BC13EEB9AD75DCB2A, Observed A51D37787BE1A112B20EFA2B8DE1F031B05EF36C18EA96DAAF5DECC5AD3B3EE2C7602785AF2 B07EBF6280058704D1B2B35583C0CAB8DC82A15E0522D22D76A0CB167446F1FC8B767194084 CD120B4E65C99570086FEA31CE996D7E8D3C7428C634D86A	None	4
212.235.98.139	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	4
37.142.68.113	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
109.64.200.194	Israel	147.237.0.121		Suspicious Response Code	Block	4
192.114.105.254	Israel	147.237.0.121		Suspicious Response Code	Block	3
62.219.44.242	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 62.219.44.242 (sigalgs DoS Attack)	None	3
212.143.99.102	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
46.116.14.216	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
94.230.92.154	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	2
85.64.103.117	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
80.246.137.42	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ctl100 in www.miluim-ishi.aka.idf.il/form3010	Block	2
91.231.193.150	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.57.50.16	Israel	147.237.0.121		Unknown Parameter ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	2
212.150.82.114	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	2
93.172.191.48	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.79.250	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	2
46.19.85.57	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
109.186.184.46	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
94.230.86.122	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
31.168.25.86	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
212.235.96.66	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
85.64.103.117	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesNames in www.miluim-ishi.aka.idf.il/changeunit	Block	1
79.183.196.78	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
185.32.179.11	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.46.36.81	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
109.66.51.185	Israel	147.237.0.121		Parameter Type Violation ct100_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
89.139.233.38	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
2.54.46.111	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
217.132.29.130	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
212.179.129.6	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
81.218.71.68	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
62.219.44.242	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.226.45.174	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.85.102	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.102 (sigalgs DoS Attack)	None	1
31.168.101.163	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
212.150.66.161	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
185.120.126.199		147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
46.120.232.235	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
109.66.51.185	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
5.28.188.242	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
212.235.13.100	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 212.235.13.100 (sigalgs DoS Attack)	None	1
81.218.176.47	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
62.219.44.242	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
194.90.89.5	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.253.196.55	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 0B7A6061B5D4D4B8A857FB8336E9439745A5C0A8EA8CF2D1CC217DF6D64EF98CC4CD393BF5 39365DB37744599603C5646D6F40277CFB8F46ABC428BE235B75F6ADFE387E1F292992EF6C028 CB582F47AD2706561CF6218373ADB9CA227B225F1855D2440C7AF66DC04E38DBA242C2FD8F 266EABA6691979818E7AE9A2F86DA59, Observed F5560CFC63BCA3AAE77FBADDD5A8AA641231E41A30C849493B2A1EFA2EE78774D7643F4C6 14B805AFEE52BAA86CEEF0B31E6B2B03B01935C30908D337D938AEAAADF26C8ADD64A51BF07 C0D2D6EBA7A99A593BF2E62C5FF55C606E776C95618CAE7F4	None	1
46.19.85.102	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
31.168.245.132	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
87.68.157.223	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
80.246.137.202	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 80.246.137.202 (sigalgs DoS Attack)	None	1
62.128.40.226	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
37.142.150.32	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 56EA7727C0E2CE5C8FE32CD944DB43CB0808EAF02ED860DF0D909F2F2D271857C87AE1823B5B 3F5DD20F5AAE6F03B9F4FE0DE2969867A3B085B2D60B7A45D83F98BE1EEDB5ED307117EA860C AB683A00B538237FA0B22EDB5367DDA976E9ABD3827E7A184D70F62091F1FE2B30A34D4FC53 A0736DD70C767E020A25805F0FE9F, Observed 77384953F7A48D1494EE5B90E32A3A5EC1403C2F3BC00E7D6CB99867C0A94ECD5204A4918E0 7A81653D7D231E579F48B4B4D87208FCE27B1BA24834AF7A4F97B78F06DE5E85DBBD104C0294 C2DA43DE3F05713753C4C871CDD41104CE6181ABA83CF0A	None	1
109.186.184.46	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.186.184.46 (sigalgs DoS Attack)	None	1
5.102.229.112	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
212.235.13.100	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1

02-03-2016 to 02-04-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.110.192.74	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.180.143.10	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
195.244.23.42	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
176.12.154.8	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.12	Israel	147.237.0.121		Double URL Encoding - parameter: returnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
37.26.147.175	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.66.51.185	Israel	147.237.0.121		Distributed Unknown Parameter on www.miluim-ishi.aka.idf.il/login parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend	Block	1
89.139.15.177	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected COA0E80B57CA0E326E90124AF1A89A9B6D1181A20C13D2B12FC78B3056E90CF73AE3D6B6BE9 FFE87DE03C7DE63441F995A69CC8D8549A2A37A364F6A07A3AE74829EDB4C77B0623DD9D55 6CFF8DF7908419DCDB446F924486440B8831B82DBF7E1B501D63C13A5DA89BB157AA4587762 752122FCE075847B41B1F57F85092FDC, Observed 7264EF4F12702BC3B6F2446BF4D043DA5C7F62AFFE3A0C29B96B8127E044B55572F299DF68357 F14F2524C8B1C32C2C35CE0434A7B0024E204D8B51DB6CDA62A2FB9260C6276370285B8C71 5D9E748BB30FE366220FFAE0B4DF1541D6ABB829C31B368	None	1
213.151.53.59	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
80.246.137.202	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.115.190.190	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1

02-03-2016 to 02-04-2016