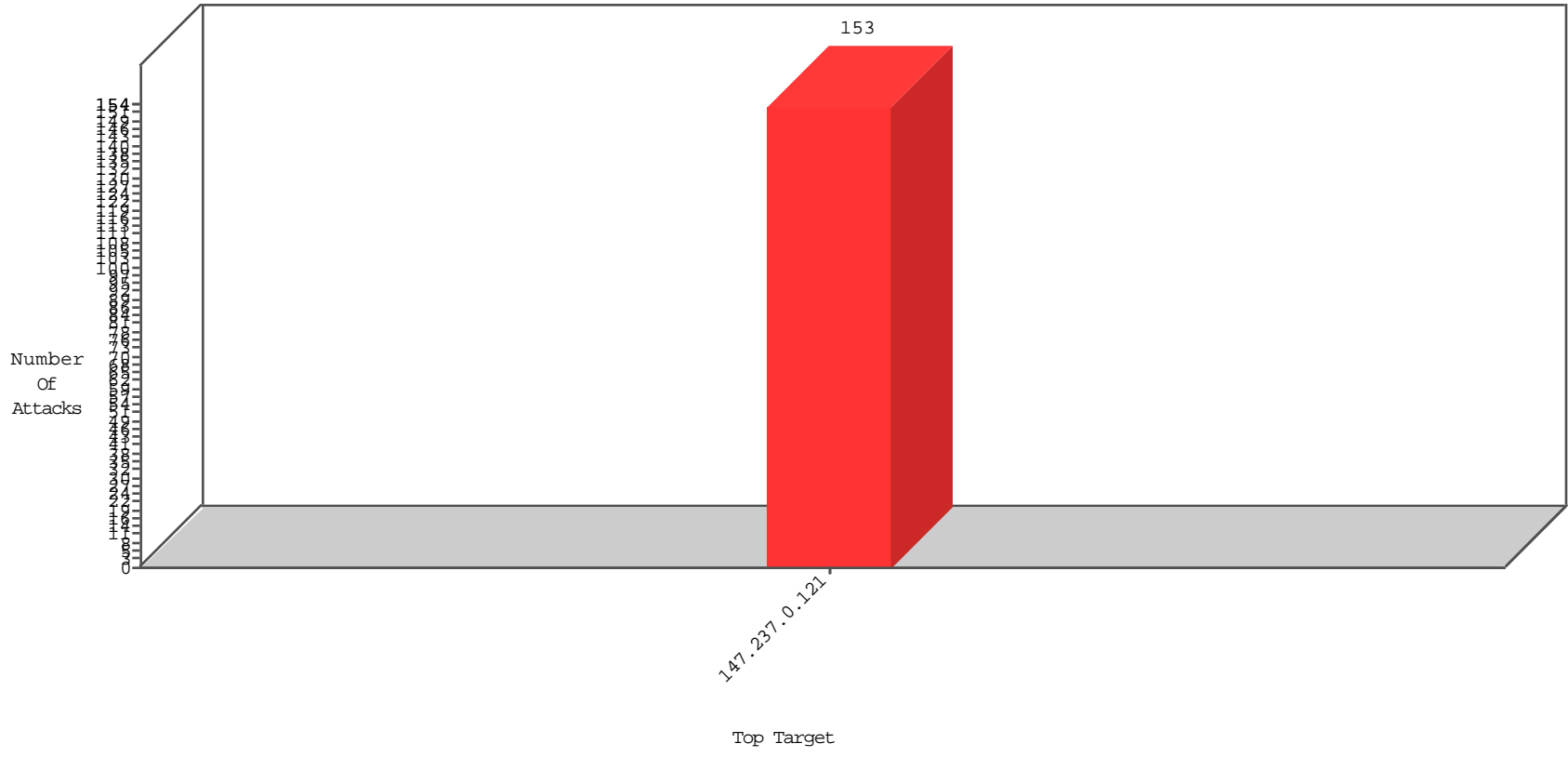


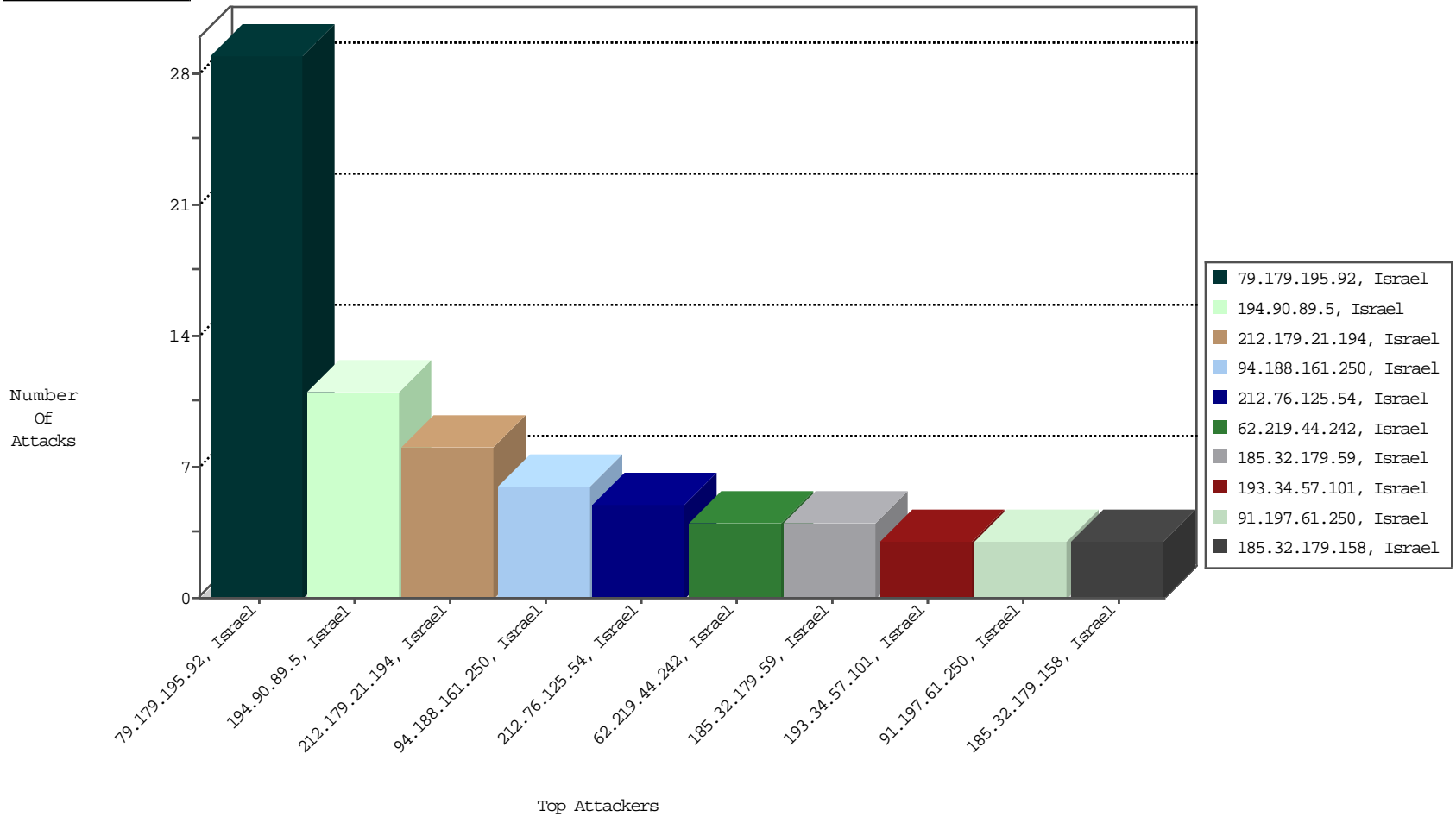
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



02-09-2016 to 02-10-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.179.195.92	Israel	147.237.0.121		Block_Udp_All_Nets	drop	EEL-Israel	29
52.28.32.164	United States	147.237.0.121		Frk_Under_Attack_Con_Https	drop	EEL-Frankfurt	2

02-09-2016 to 02-10-2016

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
94.102.49.151	Netherlands	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
176.13.16.31	Israel	147.237.0.121		portscan: TCP Distributed Portscan	1
193.201.227.65	Ukraine	147.237.0.121		ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
205.167.7.244	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1822
149.78.139.79	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1481
69.31.51.65	Anonymous Proxy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1344
95.141.29.36	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1294
194.9.253.238	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	923
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	899
165.225.76.56	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	819
149.88.253.31	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	768
199.201.66.3	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	607
165.225.80.49	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	589
93.83.89.162	Austria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	464
158.116.225.93	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	423
149.78.34.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	371
185.32.179.125	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	361
149.78.225.34	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	333
17.78.122.155	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	322
149.88.154.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	307
14.203.99.118	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	303
149.78.30.23	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	284
169.253.194.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	277
208.87.233.201	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	277
31.168.89.122	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	261
213.26.115.46	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	238
14.136.249.162	Hong Kong	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	236
149.78.23.158	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	215
167.220.196.41	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	208
185.120.126.8		147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	198
149.78.184.96	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	195
192.88.162.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	194
212.183.128.178	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	179
149.78.187.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	176
149.50.77.34	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	166
149.78.139.30	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
149.88.188.97	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	155
17.78.104.113	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	154
149.78.26.237	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	147
2.54.41.233	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.34.111	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	130
213.93.183.129	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	128
142.157.178.249	Canada	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
149.78.34.148	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	124
149.78.79.236	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	119
149.88.119.22	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	118
149.78.19.19	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	117
149.78.225.232	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
149.88.43.243	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
149.88.73.50	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	115
66.102.6.90	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	109
149.78.198.144	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
149.78.234.161	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	98

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
194.90.89.5	Israel	147.237.0.121		Suspicious Response Code	Block	11
212.179.21.194	Israel	147.237.0.121		Unknown Parameter __EVENTTARGET in www.miluum-ishi.aka.idf.il/shamapchange	Block	7
94.188.161.250	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluum-ishi.aka.idf.il/changepassword/newpassword	Block	6
212.76.125.54	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100\$txtNewPass1 in www.miluum-ishi.aka.idf.il/personalsettings	Block	5
185.32.179.59	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	4
91.197.61.250	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	3
62.219.44.242	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
185.32.179.158	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	3
62.219.131.135	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	3
109.67.133.62	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
82.166.130.166	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	2
91.205.155.186	Israel	147.237.0.121		Suspicious Response Code	Block	2
62.219.114.144	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
109.66.128.34	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
84.108.249.112	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.80.151.194	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
46.117.18.218	Israel	147.237.0.121		Suspicious Response Code	Block	2
109.64.185.23	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	2
87.69.43.19	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
31.154.29.94	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
194.90.25.122	Israel	147.237.0.121		Distributed Unknown Parameter on www.miluum-ishi.aka.idf.il/shamapchange parameter __EVENTTARGET	Block	2
91.231.192.149	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.86.148	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
84.111.208.107	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 5907A2A88BA34C5F64BD3DCDDAD95BCD026696C23B3E8951AD1A157341DE98E49636F6E8D5 F6D16C8BE34690E9043FA2001C82D6B2E8B40E61C78EA5650915AE5FBA23808D98AA818D14F5 5B55975FEA4BC12966AD3E9809FFF3C0A77774927092A7DB4804E8FFB67A2CBCC2E21A807DC 6DF6A80A8079D67AFDA75F95A06B98C, Observed D290D68B4C36731BEE871CBD7B48AD17D5885E67A4C95EB6CDF4A097921EA031DF7403D0EE6 7777A498581ED11E818580E2C2194C65F651D2F7995C89A18BEE624B234C6EEE4AED971A23FB D6A7E07F7901BB329B998C4D9F26170A99E375948AC095C	None	1
82.81.3.65	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
193.34.57.101	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value D1C3E66B0F6A690EFDB04EDA407A7A0311AB24A4B0DB2107E6273E1500F38FE886F55AC8CA5 3D63ADC7C0B381945F29D7BA5E5FFC0691744EDC20456B6AF3B295325BF8754A12E598752510 A29253396BC9828A45A45CC6748E0087646CFB139CA4F8344113ED6A019BDB14E6F01FA470F F35F7C0CFE64CEFC16FD5265A64822FDB50972E4CF7D460FFFE0E2E5B2F6353015D47CFA8780E 71E7AFF83F56E05BC1	None	1
185.24.207.32	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.49.185	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
62.219.44.242	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.65.61.17	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected CE12C4760EB841CE7DAEBC30E1BA270878D16952BC42C207FBE34D33988DC39A7B7725A618 A8D86E165035DB1E5C58841306EEDCF60D5C3EBAE5B26F8C33B2289365AA840827EE4FC80325 FD555F3192FA0121C294382CDF756CEB85A4A20DD1759641A1F44340DB8472DB34BD3056964 E55DF55DD056CEE5E102F5D1064ED41, Observed 4BA0B10363F2E76CEF1F45CD012A466A3404019933D6C33F840E95B2021430B27FA46FD036DC 14301E80868A65A76ACB909D7F3E30D9DEDE9D2BB2CDA5DCC8BFEEAE34D24DF819A68098322 5CBC3852740AD95E2B7B037D78B400B119B6BCFAF15D3B6	None	1
31.168.1.202	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 51F11446618927BFA6AF1EC200CA901BD2187E6AD9AD1B0B85FC5B142208CAF8BF9363D3950 A7332B05C6A5BD866DCD608D04DFF5433C21859D5219C88B64E0AECAAEC28ABA689C2D023 D275B1161AC5FDF64CA165EDFD0BDE21DC0F11987D76832914A9A70E9509D93130E034321D A653DC5B8F685552C1BA9198708B8784B978DE31E68FBC30632F22C7C8CA5DDA9B332A17E6 6A8B92852A4412AF0910BE70	None	1
213.8.39.241	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
84.108.238.214	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
80.246.136.253	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/login	Block	1
77.126.215.170	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
109.253.213.219	Israel	147.237.0.121		Unknown Parameter ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/smsverify	Block	1
46.19.86.255	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.47.32	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.179.148.59	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/login	Block	1
84.228.92.44	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
193.34.57.101	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 193.34.57.101 (sigalgs DoS Attack)	None	1
79.183.15.203	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/changepassword/newpassword parameter ct100\$ContentPlaceHolder1\$txtNewPass1	Block	1
109.66.121.226	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
37.26.146.234	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
217.132.45.31	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
84.108.249.112	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
80.246.139.183	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
192.115.248.2	Israel	147.237.0.121		Unauthorized HTTP Method	Block	1
176.13.1.125	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.28.198	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.90.242	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 2A311C9D48714383FBE7A3E9D8278AB28B2BD8760CC290BC4BD832999BD5F75273B2DABEC0 A78EC4429886895F3EA32BBC1DD006F1064B36C53413C84B92A2A74CDF157CC551DFD8A49C 9470B4F7A1FA87E6A0F7B5473766F1E919AFAC64D2D0345E39C4E02F5A6A716C96741BA519A 52621D0CE8446A1CD8958D0279FB34F22786D1B0661B75D8889F99DBB9180A1A26ED9104701 47AA07A193022FF494238	None	1
46.116.54.190	Israel	147.237.0.121		Suspicious Response Code	Block	1
2.52.47.32	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1

02-09-2016 to 02-10-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.199.93.129	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
85.64.188.216	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
84.108.104.201	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.108.104.201 (sigalgs DoS Attack)	None	1
193.34.57.101	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
80.178.95.97	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 80.178.95.97 (Open Mode)	None	1
91.228.248.251	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.19.86.59	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.179.21.194	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected CB99B74BC91137633F5675EFF9846633417E5DB96FD9D32A6712BFF01CC9B8E38A0DBA806348 2D37409E77E572F9BAF346CA94B1C68E1A89DDF37B479DD2DAB3DF8D81B50321951427531C8 1017F4031CF7F22FA79CEF227E86590B0A8E1A65B7B20BA45BCC449917E331CC95A4EDB4B719 C2D2A245D8990F35B6BE9259254D7, Observed DDDF1083CF9AD7D80997B426C1481FFF50B1F70F2B68E61F99A8357BABEB24B3F8C40A46E53A A9C33D9C233FEA18DD70D3DE32798EDF4087359827D296F7E0CB408CFDC1B5B7C850DE1FE07 7F9FF4FC139B6B3E225C3CCFDCBCDA2CDD841C26765977F	None	1
192.198.151.45	Europe	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 360294E6BD851EE74E3C760903C4A66B83E067A8B8FE7F80EE4BCD12FC44D8F12BAB738947F3D 70C7AD990B6261D5589EDC9A915C8649FBE386595C224C9DBCE182A0B6A986A726FD441666 47ABC6DE852B7743A18B583ABD4510B797A79A79456B144DB16674D80168FA21C381927F05 9B2F21D190350994A66EFF43C344761, Observed 425FDF7E5C1B1336A2CD6209F0E55DD4034CB4B3BA03A386324A6C1CE13008A5AA0F593E08B AF2A227194AC54DA79F4CA400CF9FEBD3B469B910ACE2A00565E761FB1BA589AE6185FCDAF7 A0A468DE9F577C72FC1E348A2A33EBD64C81EB6EDFCFB6BC	None	1
176.13.22.189	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
79.180.113.178	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
212.199.177.34	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
84.108.104.201	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
188.120.154.220	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
80.178.95.97	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1

02-09-2016 to 02-10-2016