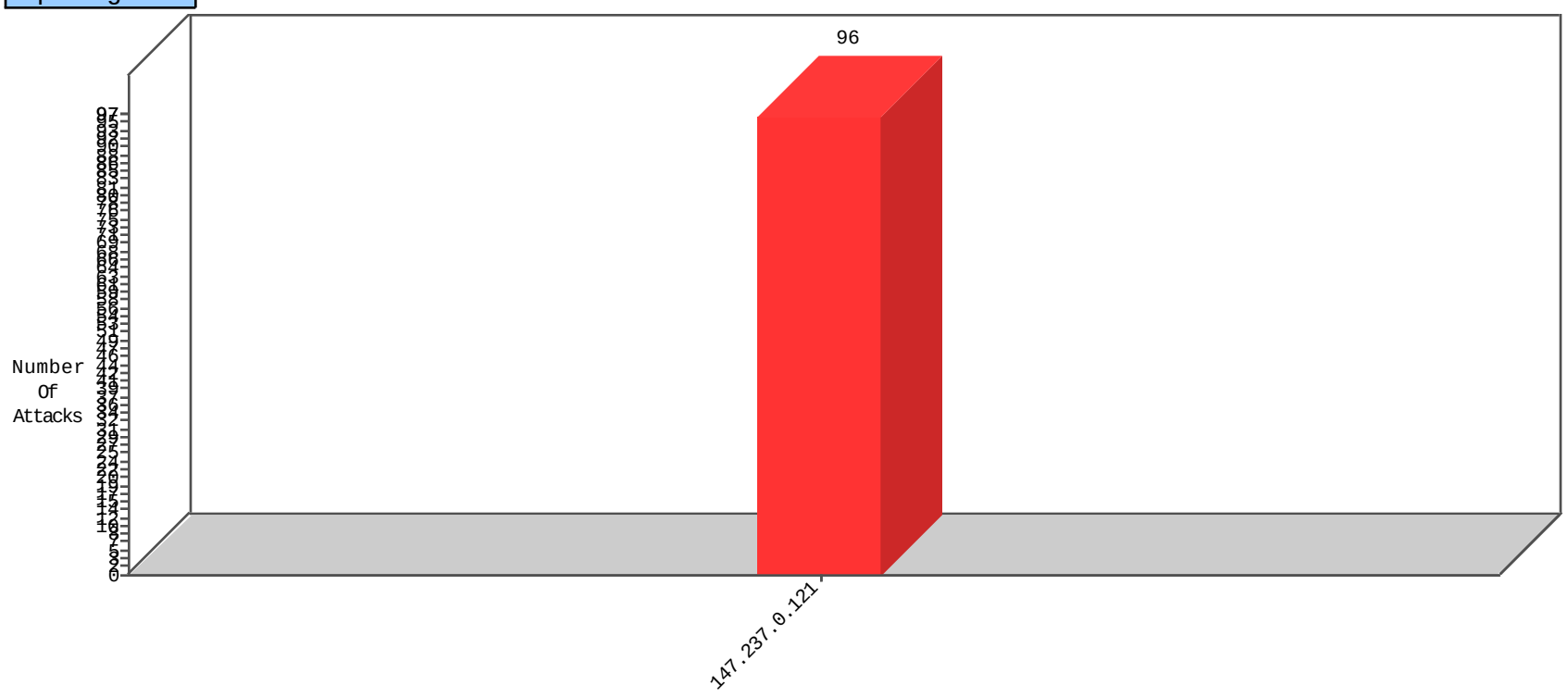
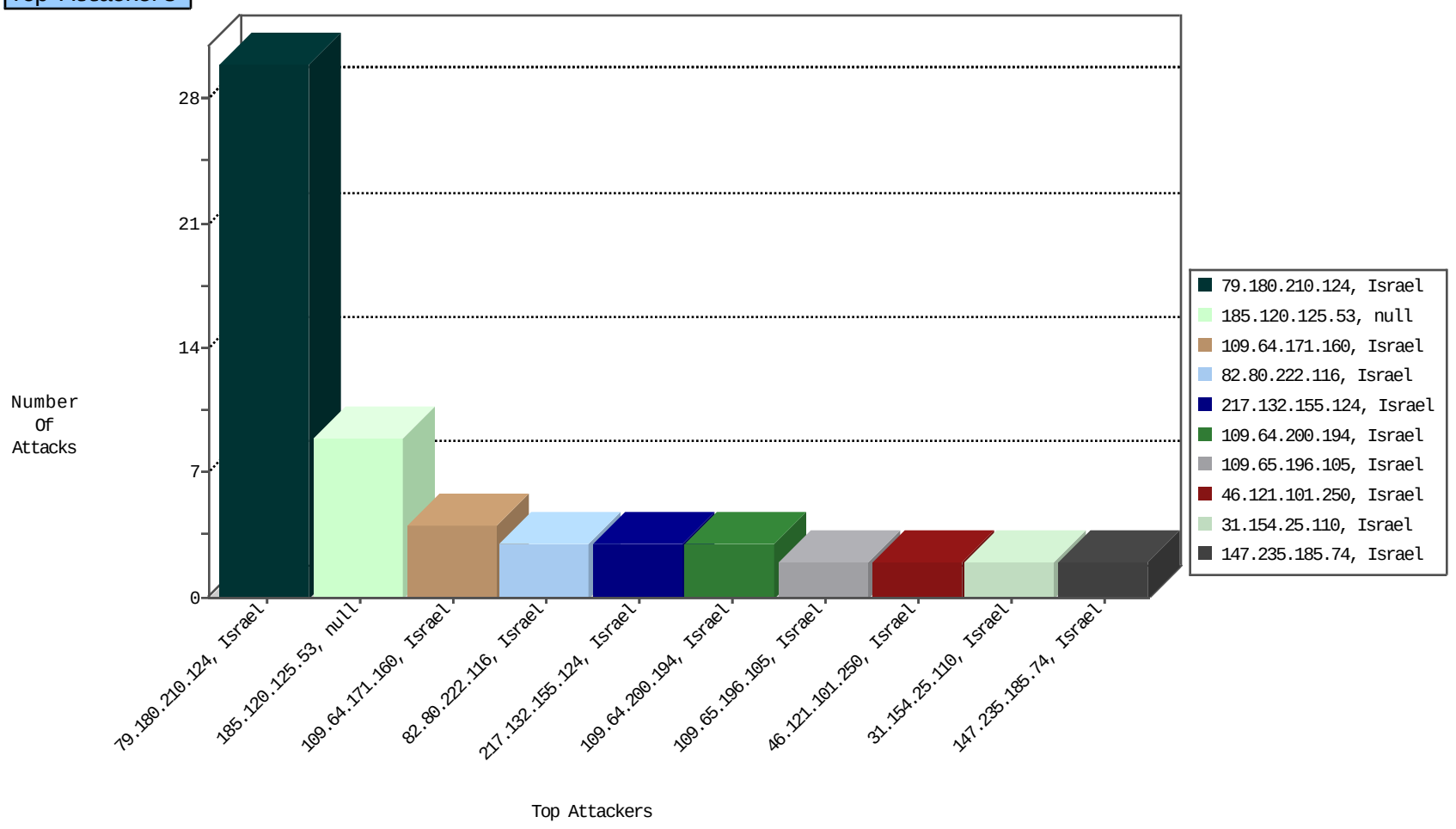
01-25-2016 to 01-26-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-25-2016 to 01-26-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.180.210.124	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	30

01-25-2016 to 01-26-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-25-2016 to 01-26-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
78.193.2.8	France	147.237.0.121		ET SCAN NMAP -sS window 1024	1
183.60.48.25	China	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
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
93.198.70.229	Germany	147.237.0.121		ET SCAN NMAP -sS window 1024	1
183.82.106.200	India	147.237.0.121		ET SCAN NMAP -sS window 3072	1

01-25-2016 to 01-26-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1555
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1552
194.42.67.50	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1535
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1150
213.8.87.137	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	756
149.78.24.9	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	543
149.78.49.182	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	496
149.78.251.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	442
155.56.68.216	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	431
192.117.129.95	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	333
85.158.139.101	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	305
149.78.250.197	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	301
50.240.212.81	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	288
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	223
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	222
84.94.198.136	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	189
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	181
149.78.169.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	168
79.180.210.124	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.122.68	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	144
149.78.253.24	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	131
149.78.39.205	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	130
38.127.167.45	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	124
149.78.216.50	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
84.109.105.15	Israel	147.237.0.121		Bad TCP sequence		monitor	100
64.41.200.101	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
149.78.237.221	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	84
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
149.88.52.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
66.102.9.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
149.78.138.203	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	67
66.249.64.175	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
66.249.64.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
192.115.177.202	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	58
149.78.39.191	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
85.158.139.107	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
66.249.64.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
27.55.234.221	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	47
66.249.83.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
66.249.83.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
149.88.146.87	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.78.63.20	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.120.125.53		147.237.0.121		Suspicious Response Code	Block	9
109.64.171.160	Israel	147.237.0.121		Suspicious Response Code	Block	4
109.64.200.194	Israel	147.237.0.121		Suspicious Response Code	Block	3
82.80.222.116	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
147.235.185.74	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
217.132.155.124	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 217.132.155.124 (Unknown SSL Session)	None	2
109.65.196.105	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	2
46.121.101.250	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
5.102.254.72	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
82.80.222.116	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected BAE0223BE585396F2CF822E544B6EF9EEE79FB53577292EB12D6353B53C0E2BE3A5475182B8F625E0C3A4284B55E2DBC2A4D9C71D8CD8CBA9CDA1C8B82B114B1DE8B63E61BB9317DC3B05DC63DB1BC93DA9E318253A457FE36BE205CB6A37A6CD590CC393BD6E5CAD16C2F524F2AC5E82C5F036233ABED708DB3D0D313F01B96, Observed 85ECC6E38E10F83D7EB2C1CD0A39E79875D798E593361571753197004E59AAEC0328CC07319DF39FC77885C1FF07D9AB9AD3C40438D3927313E68C2B0499DA2F2454F3C061E3088C1B6CAFB4EAE8D949AB242370A4F759DEDDFC62C59206C0CA85E0D5	None	1
46.19.85.41	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	1
213.57.27.82	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
176.228.217.6	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
109.65.210.52	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/l	Block	1
84.109.208.132	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.179.17.248	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
31.154.25.110	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 31.154.25.110 (Unknown SSL Session)	None	1
199.203.215.1	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
132.73.193.103	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 3F5572A9DDB4C008D4E31FF349C1C5C949D3CD3F8D409FC3FD6C0432AC8374ED8AF8651B65ABAF4952B2FC60AA89D5B78F9F1009B723FFA8498E0FC99391B5E60E41343745935613199CAF4C66F2606E225033D247CF0F1700225D4DC67632546728DA5F693EBB586D3924BAFB711E6C09EE202D903C99CB8D51169964B37269CDFFB05AF4DCE851DA4E05590F06D1F4D3FC0DDC903AC8C16E8920E8E555BB1B	None	1
109.65.184.15	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
46.19.85.245	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
213.57.156.246	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
109.66.140.224	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
93.172.19.60	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/password	Block	1
80.246.137.63	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
31.154.25.110	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
212.179.23.29	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
109.65.189.39	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
84.109.105.15	Israel	147.237.0.121		Parameter Type Violation ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.24	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
192.114.38.14	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
2.54.57.48	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.253.147.177	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
82.80.132.60	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected FC8FBE3EBA5726FE8FD81648C867A2795D89318EE0B4A45B7C6765D0707735C994FEC3DD58CE253DF507A8FEB065E40A481EB26F96AE3BF43E5841BD49786938728BA3167E016CD3AB968DE0FFCF679F4AC419F730EAD4DC4D22823D8CA5FDF0868AD8B022D3988EB37532C913D34B93E4F29F1C521B660CFE98DFDDFDEA4E9A, Observed EE63E2F0DD4FD00B46989829295612E8FE26641E4C54AC3EAF88F99D575C416B4D128B4A067445F9F86DF155FCEE938CBBBE8283B5BD64A2EFFFBE4A1B4058B078658F1AB1CCF47F0845C8B34BDFADFFBF989424365768787D504F51F864CBEDA467AF	None	1
37.142.68.59	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
212.235.91.76	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
176.13.21.252	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.105.15	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
217.132.155.124	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
194.90.76.218	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed BF2D3E23A4B01DDF750B6155221A6BB5427F887A3666E59B32BEA34DE8426408C713F70100E8319DC8E9F204F0E96CC2623CFDABB0F8637429B4D7C77010A95A554BBC07167E3528B046AE08274116A7623B8A0AE509E6D5C665418AD8F655B04E8A8FC16EC481B1A449B90CBD02F654559F346E1AC3A348AA3C65382BD48034B4EC6FFF5ED6276A95CEBAFFB6209BB1A694A021BA3D0264990D370F71710A30	None	1
109.253.207.249	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1