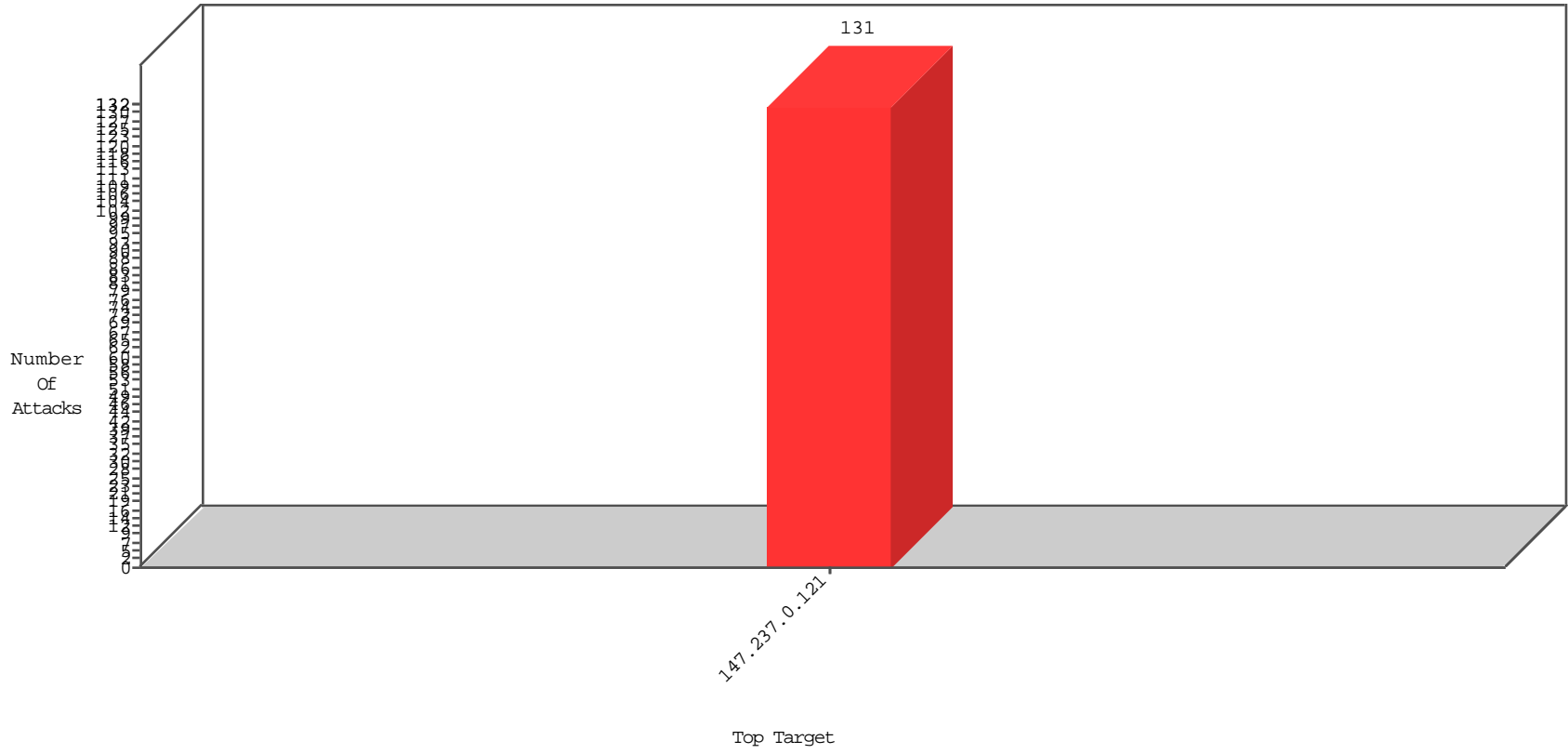


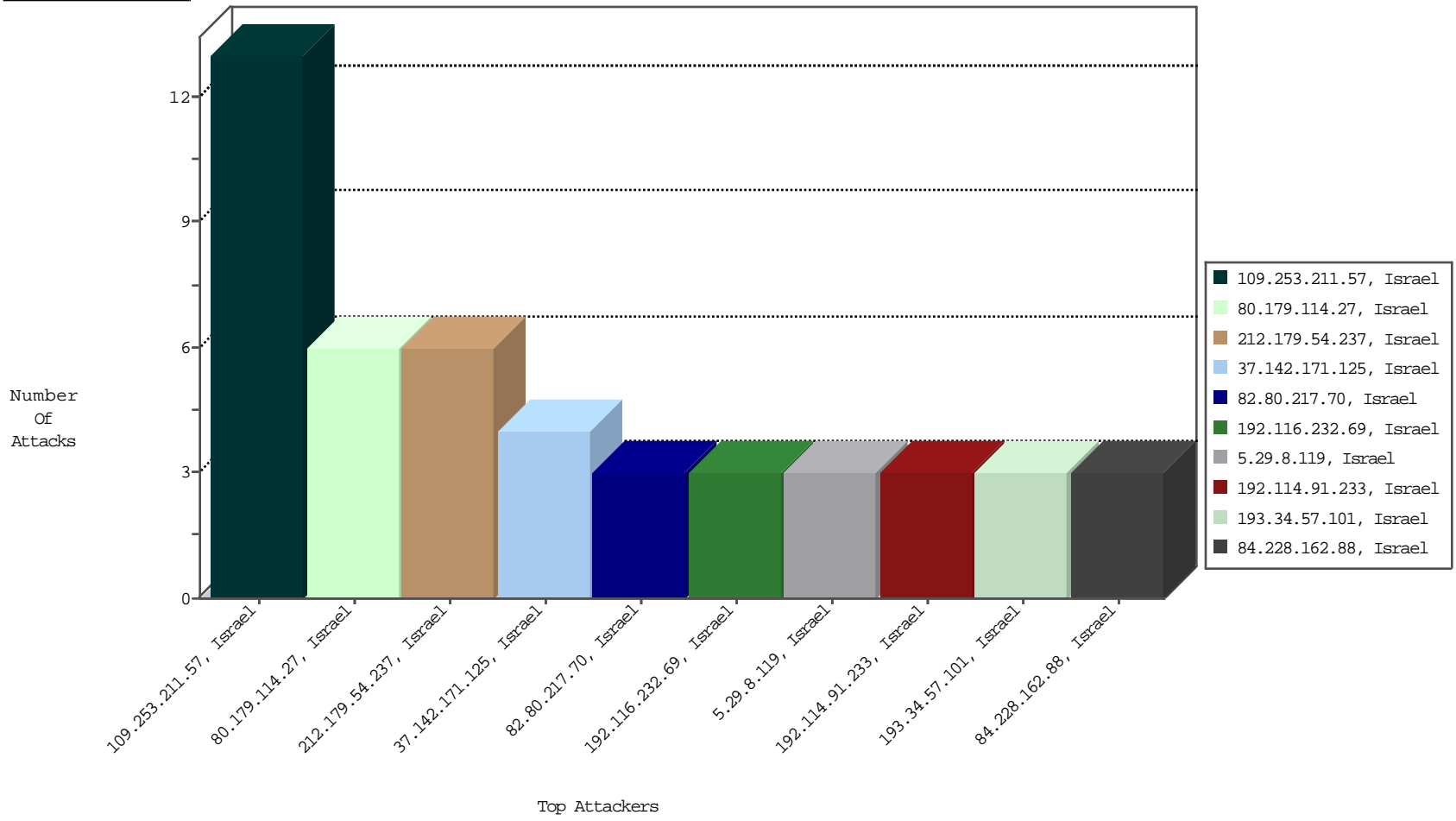
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
109.253.211.57	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BEL-Israel	12
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	6
82.80.217.70	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
187.188.120.123	Mexico	147.237.0.121		JLM_Purple_Con_Limit_Http	drop	BEL-Israel	1

02-01-2016 to 02-02-2016

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
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
80.82.64.190	Netherlands	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
122.144.178.145	China	147.237.0.121		ET SCAN Potential SSH Scan	1
115.29.224.200	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
185.69.53.105	France	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
149.88.41.147	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	2592
205.167.7.247	France	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1738
17.78.96.188	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1400
217.194.159.14	Satellite Provider	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	885
17.78.83.134	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	808
216.185.39.196	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	768
149.78.175.229	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	605
149.78.169.83	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	521
87.121.106.17	Bulgaria	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	492
149.88.154.143	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	488
17.78.122.195	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	459
46.19.85.117	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	405
149.78.138.29	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	372
149.78.46.89	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	364
149.78.56.7	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	362
199.207.253.96	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	348
81.218.146.181	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
62.168.56.1	Czech Republic	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	320
149.88.20.224	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	296
194.208.45.108	Austria	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	281
149.78.253.144	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	238
149.88.20.70	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	236
149.50.77.180	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	214
63.163.107.100	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	212
192.88.162.1	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	209
149.78.20.96	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	180
149.88.70.187	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	165
149.78.22.214	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	144
37.46.39.99	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
97.107.115.20	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	137
149.78.241.105	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	125
17.78.71.138	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	124
149.88.147.99	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	124
149.78.194.156	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	122
167.220.196.205	United Kingdom	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	115
192.176.1.90	Sweden	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.88.126.94	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	101
149.78.198.144	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	98
149.88.29.192	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	93
149.88.201.246	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	90
149.78.240.146	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	90
80.246.130.158	Israel	147.237.0.121	Bad TCP sequence	SYN retransmit with different window scale	monitor	88
149.88.203.223	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	87
149.88.69.90	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	87
31.168.96.254	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	84
93.73.2.157	Ukraine	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	76
149.50.71.237	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	74
149.78.34.82	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	74
149.88.223.105	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	65
213.126.106.206	Netherlands	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	65

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
80.179.114.27	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	6
37.142.171.125	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	4
84.228.162.88	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	3
2.52.47.107	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	3
192.116.232.69	Israel	147.237.0.121		Multiple Unauthorized URL Access from 192.116.232.69	Block	3
79.178.115.86	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluum-ishi.aka.idf.il/changepassword/newpassword	Block	2
46.19.85.168	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	2
194.90.225.101	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/lobby/	Block	2
5.29.8.119	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	2
87.68.37.166	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	2
2.54.30.134	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	2
193.34.57.101	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.144.253	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	2
176.12.154.242	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
109.186.180.36	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.186.180.36 (Unknown SSL Session)	None	1
62.0.53.242	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
217.132.119.94	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
37.46.39.99	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
212.179.21.194	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 212.179.21.194 (Unknown SSL Session)	None	1
84.111.14.63	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
80.246.140.100	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
193.104.115.2	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
192.114.91.233	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value A89900F112844F5209281EB2CD170E7D6E492B94EDB5EF5C19FD2030FDD9BBA4837207C2FA77A4F7D0D12809C1B4BBAA78B13EC82BA4BE3863A9F0F14FF25B7CA3D2249AC0463B99A0C2E0227B7773E8A299266A5EFC599220CA72AB4B003C91111D84F94B0DF90466B14AEC6A57AAA160BCD8797C32941EE48ACC1150AAAFECF98F4398157E13002FCB035828DDA34534DDC6D24C358B30C751AA2B3F7F337F	None	1
79.183.153.198	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
109.253.210.101	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
77.127.215.138	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	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
95.86.84.73	Israel	147.237.0.121		Multiple Unauthorized URL Access from 95.86.84.73	Block	1
84.108.5.185	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
5.29.8.119	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesNames in www.miluum-ishi.aka.idf.il/changeunit	Block	1
212.25.81.122	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
192.198.151.44	Europe	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
80.179.200.35	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.179.131.238	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
176.12.155.63	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 176.12.155.63 (sigalgs DoS Attack)	None	1
109.186.180.36	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
62.90.76.107	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/newpassword/	Block	1
212.179.21.194	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
81.218.195.187	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
192.114.91.233	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 192.114.91.233 (sigalgs DoS Attack)	None	1
80.179.37.129	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
79.177.22.89	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
109.253.211.57	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100 in www.miluum-ishi.aka.idf.il/form3010	Block	1
46.19.86.56	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
213.151.48.99	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 213.151.48.99 (sigalgs DoS Attack)	None	1
109.67.22.89	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.67.22.89 (sigalgs DoS Attack)	None	1
84.108.39.118	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
212.25.86.242	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
193.34.57.101	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value 8E19082E3083E123680225D936D17E71CDD231DFFD0E46853F125C659EA3B08285B6E76501B70E9FDF4A6300C976404E13946EA0F85D2B1A1F822D24846D5D1E2C91ED33360E767E398886216E0F74D29633BD20E707117D7BF4A921045210F60CC01796F0CF16C0C55BFB24E3DB54C8DB19F750B232AAB07C171CB085DD8440FCF5A1A460825E755837D060CBED9A7A9903B85660937511C105167526D97C32	None	1
80.246.136.185	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
79.181.173.133	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
176.12.155.63	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.186.184.46	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 83ECB88353C24B65FF6D926403B110D747233A6812596F6BBB08168528BE5416BF6AE07C2884A377CE350884596E419591B8642B86E32B13AB9679B1D3AFC636387258F71AB995D56CB374AB7B10475EAFDA1AE1249BB0BF543F1468EA97BFAB9CC9877A17AC7870C5B7887FF97BCF12182E0ECCF00C8F21CC5FD5BCCB17BF8D, Observed 7BAB47C533C011A19D2D95FCA564B206FE4D57B8CE69527682AFFA2617ECC615C2CFBAFD7E637003D095C4ADA1E8C551151B4F702C8BEF40915C76C0E3E6E9BBABFACAA8836F98CB5F3231BB6E08EFD4E5DBB9D23362A4712DF3964D16AB5A86FED750	None	1
77.127.32.112	Israel	147.237.0.121		Illegal Byte Code Character in Method	Block	1
46.19.84.23	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
212.199.71.94	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
82.81.58.40	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
199.203.100.145	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
192.114.91.233	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.177.56.93	Israel	147.237.0.121		Parameter Type Violation isCharig in www.miluum-ishi.aka.idf.il/login	Block	1

02-01-2016 to 02-02-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
128.139.28.8	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceholder1\$txtPerutBakasha	Block	1
109.67.22.89	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.121.247.2	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
213.151.48.99	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.76.121.93	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
84.108.182.203	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceholder1\$txtPerutBakasha	Block	1
31.44.139.97	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
80.246.139.124	Israel	147.237.0.121		Double URL Encoding - parameter: returnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
79.183.125.79	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
188.120.148.188	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
77.127.32.112	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.74	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
212.235.98.139	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/newpassword/forgotpassword.com	Block	1
93.173.235.199	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
83.130.113.105	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
2.54.169.60	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	1
209.88.198.1	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 76C8A8B258A3941B7EB9D852EDC058BF1A9FDCBEADDE5088E35F515AA0C4CCEC42C2E3D90F2B0AB4A2A6C59F0998705BEE03AD55394BB9EE2DB472F3C7B8B3C1F9AC723591A1E8243753A9636E10AAF25C104DAE70D5500F756A90127A521A9699F8456180D780DE47C44BD1A2922C64E1DC26860FB29076D236F1F7CF68D04E, Observed 111A18B15AF439480A40138FD464A3537B5B3FC839C39935FA072D6E097D200CEA2940D0BE963A863F1C6AB038336584913CFC95132C56394843B259C1029E77D66849C1839535A619D3F9E73EC9689C94FBED21C81B7C2B6E8EAF050F3687A6FA9979	None	1
80.179.200.35	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 80.179.200.35 (Open Mode)	None	1

02-01-2016 to 02-02-2016