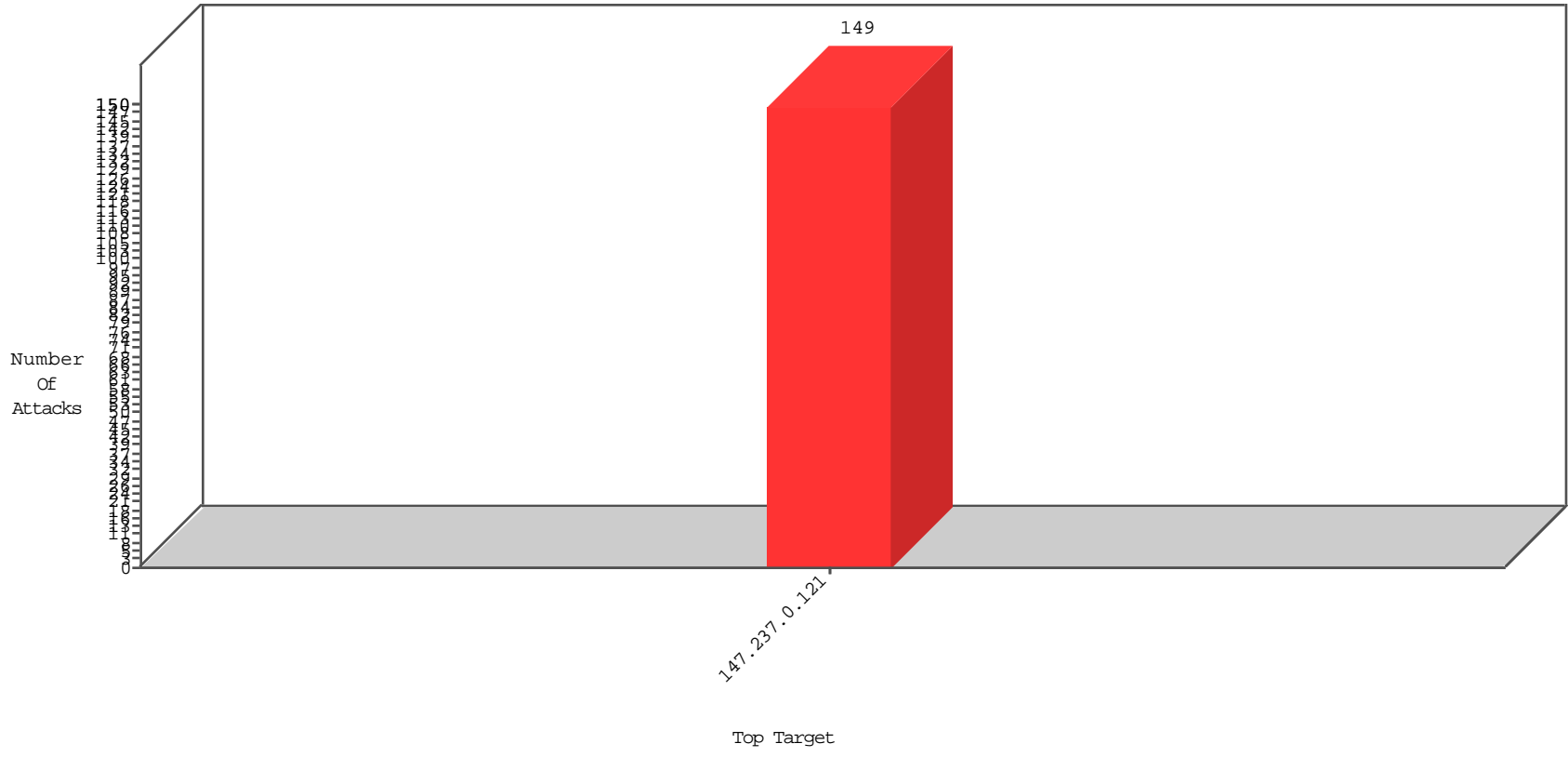


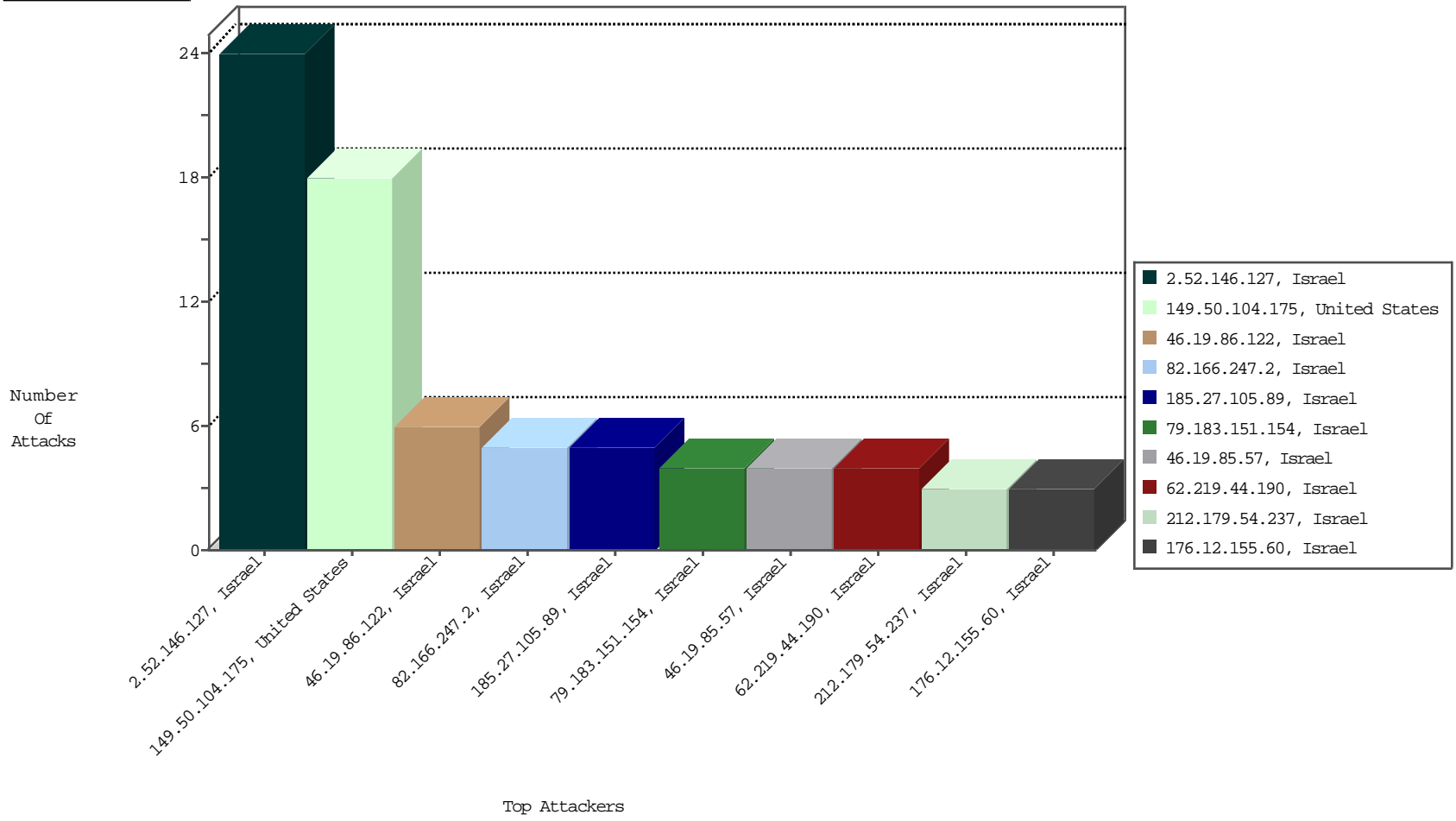
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
2.52.146.127	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	23
149.50.104.175	United States	147.237.0.121		Invalid TCP Flags	drop	BBL-Israel	18
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
185.130.215.4		147.237.0.121		L4 Source or Dest Port Zero	drop	DP-Tehila	1

02-02-2016 to 02-03-2016

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
115.29.224.200	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	2
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
145.255.2.133	Russian Federation	147.237.0.121		ET SCAN NMAP -sS window 1024	1
185.130.5.196		147.237.0.121		ET SCAN NMAP -sS window 1024	1
222.186.42.206	China	147.237.0.121		ET SCAN Potential SSH Scan	1
183.12.148.73	China	147.237.0.121		ET SCAN Potential SSH Scan	1
218.246.0.97	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
17.78.98.80	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	2388
149.78.22.241	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1455
192.88.162.1	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	745
208.87.233.201	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	671
199.207.253.96	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	592
149.78.24.145	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	585
149.88.138.75	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	448
149.78.169.83	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	434
149.78.24.61	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	322
149.88.152.104	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	284
217.33.23.241	United Kingdom	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	270
169.253.194.1	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	267
149.88.101.173	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	257
167.220.196.205	United Kingdom	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	247
149.78.175.229	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	244
149.78.212.236	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	217
149.78.95.217	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	210
46.116.42.42	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	208
149.88.49.221	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	207
149.88.221.33	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	197
149.88.27.8	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	193
149.88.154.143	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	188
149.78.44.208	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	178
149.78.225.6	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	170
73.49.59.148	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	163
80.246.137.183	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
207.232.21.105	Israel	147.237.0.121	Bad TCP sequence	SYN retransmit with different window scale	monitor	161
50.204.67.242	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	155
149.78.6.243	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	153
46.19.85.211	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.88.79.147	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	144
149.88.69.90	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	142
79.177.130.228	Israel	147.237.0.121	Bad TCP sequence	SYN retransmit with different window scale	monitor	140
194.180.84.134	Germany	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	139
149.88.45.145	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	134
149.78.104.20	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	133
149.88.30.88	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	129
149.78.199.212	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	126
149.88.4.229	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	120
134.191.244.2	United Kingdom	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	119
149.78.225.8	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	116
149.78.192.193	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	110
46.16.142.100	Cyprus	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.50.80.108	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	97
192.115.177.203	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	95
149.88.238.102	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	94
149.78.26.251	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	91
149.78.34.82	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	90
69.203.112.149	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	89
149.78.36.137	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	86

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.183.151.154	Israel	147.237.0.121		Suspicious Response Code	Block	4
62.219.44.190	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
82.166.247.2	Israel	147.237.0.121		Suspicious Response Code	Block	4
46.19.85.57	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	4
176.12.154.204	Israel	147.237.0.121		Unknown Parameter ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/smsverify	Block	3
176.12.155.60	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	3
46.19.86.122	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.122 (sigalgs DoS Attack)	None	3
46.19.86.122	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	3
213.8.245.50	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	3
79.177.130.228	Israel	147.237.0.121		Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.177.130.228	Block	2
185.27.105.89	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	2
31.168.241.176	Israel	147.237.0.121		Suspicious Response Code	Block	2
109.67.159.125	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
84.109.184.33	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.27.105.89	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	2
164.138.115.168	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluum-ishi.aka.idf.il/changepassword/newpassword	Block	2
212.143.99.102	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
81.218.40.194	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
46.116.125.69	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
109.67.39.114	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
5.102.197.46	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
212.235.98.139	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
84.109.32.135	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
192.115.248.2	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
147.235.185.74	Israel	147.237.0.121		Unknown Parameter zi in www.miluum-ishi.aka.idf.il/login	Block	1
91.231.192.149	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
2.52.146.127	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100 in www.miluum-ishi.aka.idf.il/fom3010	Block	1
213.151.53.59	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 662EA5B0AC49A004A35E182EE726C7509D778B6DB38F3C3F6B825E7D41AA3CCE599F56402CAF7AAA461A76132D12E843C125D164EC9990CD238BD2AE88E66984908D0895F498BE31BDFF0C9988D87F80B9264D9F052D079A0CE00F0CA99EF8A187DF12372310DDA0121ED7FE7BFD4F60AE0D482B2BE406353948F82CA630800E53C4E45AE964B7D6D8138BC69147B3FB0271C8BA0A2AC037D24C699E73A8EC3	None	1
212.143.136.179	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
82.166.247.2	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100 in www.miluum-ishi.aka.idf.il/fom3010	Block	1
79.178.11.5	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100\$txtOldPass in www.miluum-ishi.aka.idf.il/personalsettings	Block	1
185.110.111.136		147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
176.12.155.34	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.120.232.235	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
213.8.204.68	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
80.178.157.42	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected C4AA1778962D08D32656D974CEB124758A836583CCC5A4FA372441530B952EC94FD71146AD99FF34871B9F4A95365AAFF338AD0E9F28146C15096BD82EC03C0AF008EA1C298A60BE3CAB476B08672DCDAFDA33C7E40ABB1CB606D51F719562EC6535DC985448548341808DC33F4737346E19DE83608D037CB60F67E2D80E59CD, Observed A1C36030985857C1E1A0717D146C8E0B421D8A6A11DAD13C657ABA1138E52F4D972B66233028E95182F0B835E9A17FAACF10580686FF980F637588D1EFD4F6CDF5326640D60960E3F2CDD0F270566533302D552CABB34D3D434E8F55A8EB6E96D34DA	None	1
192.118.78.57	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/rules.abe	Block	1
62.219.129.19	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 918516323BCD21B1C451708275A24C2C86C3D6A4B7C5255E9D72834E2D6D3B29C175BE82E6EE2C3D22410871337C86C130420B3A626CC345178246F6AF96F6175CC3BC49159CDD8B43411AE872BFE0E580CD9131B2D4BF5A626F6B829676D3B0E313EB66FA08E48C0F4D00DADF22BCAC0E958E0C485BB001FE31F48C12A75398, Observed 7930759C1489362ACC12A27541A8E3E52C20EB7759D4AF08F275B810CE9F577BDE2BE2FBC74B889A1CB5A200128213862893597F2405ACC08F92A619D49CF9D6C824BCFD3DAE26CD8C18A6D36048CE89D101B25438F9BCA36418E28F945C71E7137C4	None	1
94.230.92.172	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
2.54.4.138	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
213.151.53.59	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
212.179.21.194	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 4B0D437FD0A38AE0FE5196907E3748F85DF6BD01B6B2F64980289E09ADD95A32F479C2F5C8366EE23314C4DE57E3F3C0A6E5CCBA25187E4CC0C2D819550DCC25A51D79362DA10E8DAD9F0C8E00AEB4386AFE5BB6BC366B38268032770AE2708CECE10C4A4376512992125354B5D3BBEAEDEB806F01400259EADB0298AE30516C, Observed 24B8AA88D950606870BD5320D5C2B65BCCF00783788C98A696669CF53B097EE5EC4DEF10FCFD77F6A7FB19FF67B1B33C39DD8424C0FF93D2EB1E9069368541FE0AB2D219F445DB646AB278BCF17FA0AEDDD211C991FBF3A3A13076DE18B588AFDF60C	None	1
79.178.34.234	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
188.120.148.229	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
176.12.155.34	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.240.2	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
37.26.149.237	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
132.64.212.154	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
89.139.71.21	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/login	Block	1
195.250.33.251	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPass in www.miluum-ishi.aka.idf.il/login	Block	1
80.179.196.45	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1

02-02-2016 to 02-03-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.27.105.89	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
62.219.198.6	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
46.19.86.134	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 9088409ED819B488FB3BD4170C3E01F35E809BD67381441A38382D9692874329BF110086857FBACB2DA9301550CBD09A65A678573DE2EF2ACF79F194B2BF796244DAAA008038861F76C8F988E54C7D494C40B0CA18912ECDEF4810CF14C843D67A631E0F6E10689FA6415014DD29EF2A02F4969C6CFE0F7B0085D750D55468E4, Observed 65714D3F86F5093186FBBAC9AF85E0267B49AE03C0C9B2A128496B1AF64BED33660366B03C703F04C2624152BE784BBB4590B86C2CB64FFF5EC44EA4C69B827ACC9C53D4669ED546BF2DE0F085906B94CB78BB3F17414ABE1E3990A2BAC722317B5D59	None	1
176.12.154.134	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.66.171.36	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
2.54.178.21	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ctl00 in www.miluum-ishi.aka.idf.il/form3010	Block	1
212.179.21.194	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
83.130.113.105	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
79.180.141.176	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
192.114.7.2	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
176.12.155.35	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
62.0.67.123	Israel	147.237.0.121		Unknown Parameter zi in www.miluum-ishi.aka.idf.il/login	Block	1
132.72.138.1	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
91.205.155.186	Israel	147.237.0.121		Suspicious Response Code	Block	1
213.151.51.62	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/newpassword/firstlogin	Block	1

02-02-2016 to 02-03-2016