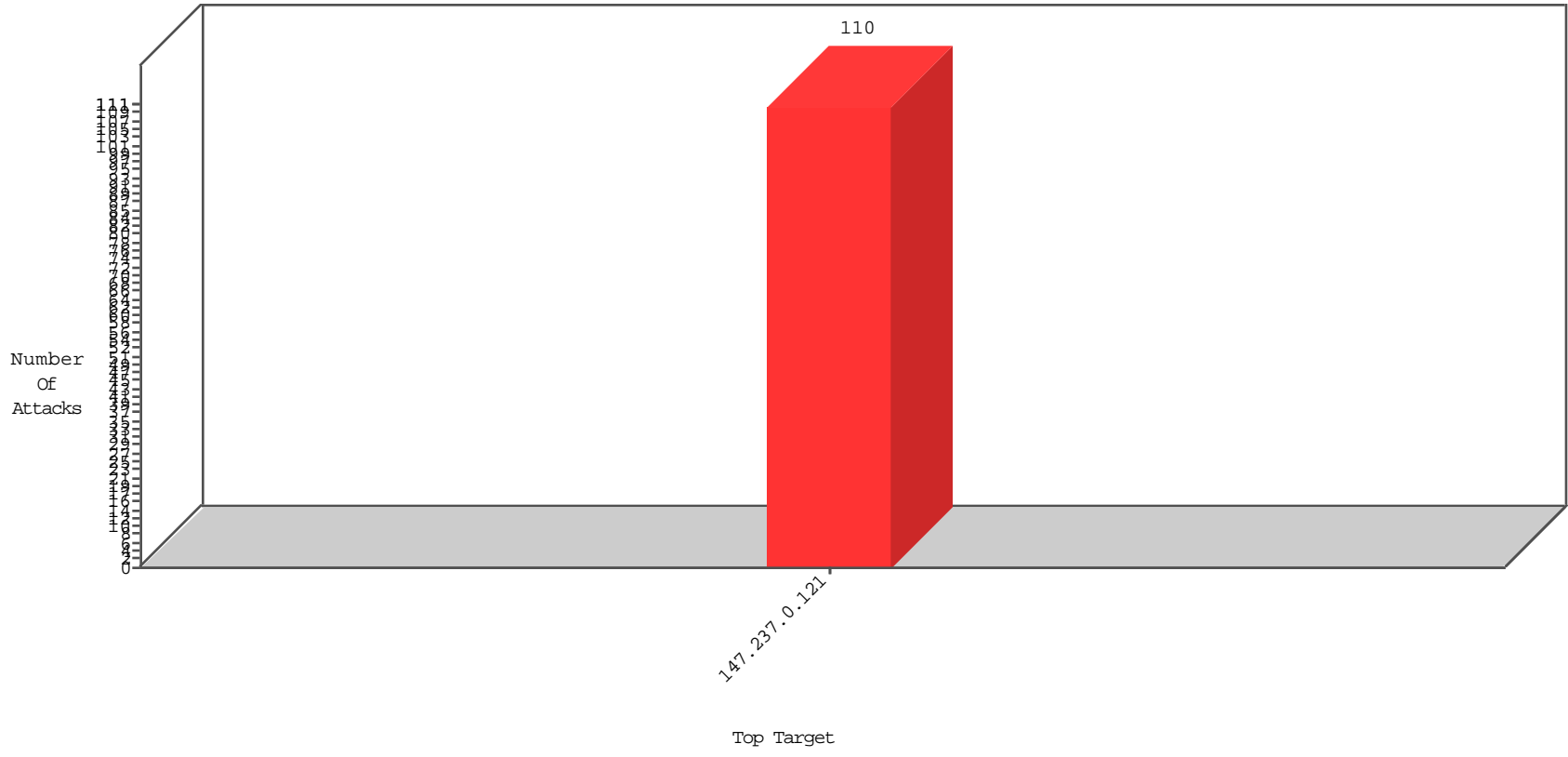


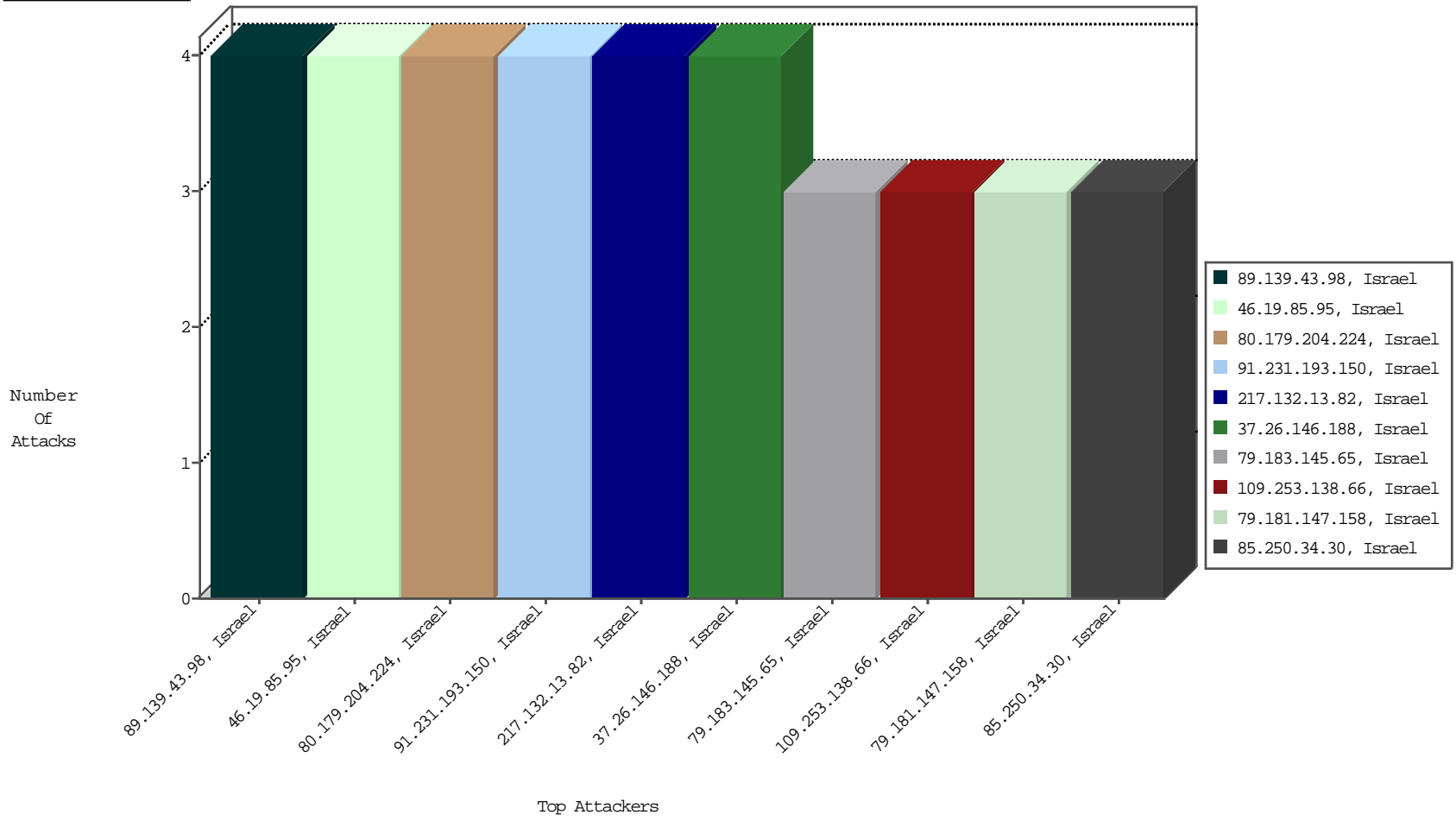
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.181.147.158	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
184.154.114.140	United States	147.237.0.121		Frk_Under_Attack_Con_Tcp	drop	BBL-Frankfurt	2

01-26-2016 to 01-27-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.120.126.87		147.237.0.121		13840: TLS: OpenSSL Heartbeat Packet	Block	1

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
162.222.185.165	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
220.231.195.122	China	147.237.0.121		ET SCAN NMAP -f -sS	1
220.231.195.122	China	147.237.0.121		ET SCAN NMAP -sS window 2048	1
93.174.93.130	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
220.231.195.122	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1
89.163.148.90	Germany	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
80.178.218.153	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2707
213.8.87.137	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1953
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1797
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1553
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1517
167.220.196.175	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	936
149.88.142.117	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	926
50.240.212.81	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	874
149.78.41.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	674
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	485
149.78.105.139	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	468
149.88.242.30	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	460
149.78.181.43	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	440
155.56.68.214	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	432
149.78.32.79	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	432
149.78.18.252	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	426
149.88.49.127	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	399
64.25.27.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	394
155.56.40.47	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	370
149.88.160.18	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	353
134.191.232.71	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	270
149.78.49.182	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	260
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	239
149.78.24.9	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	238
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	232
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	222
149.78.235.119	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	220
91.102.41.26	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	206
17.78.82.219	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	192
149.78.243.170	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	183
208.87.233.201	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	175
149.78.233.103	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	169
75.112.167.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	164
193.43.158.229	Austria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	152
17.78.98.182	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	143
185.127.10.35		147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	124
149.88.27.172	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
87.250.253.68	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.45.128	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
149.78.39.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	94
149.78.253.24	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	86
155.56.68.219	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	81
149.78.249.133	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
149.78.231.157	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
217.140.96.140	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
149.78.229.80	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
192.146.4.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
37.26.146.188	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	4
89.139.43.98	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	3
109.253.138.66	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	3
217.132.13.82	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluum-ishi.aka.idf.il/changepassword/newpassword	Block	3
176.13.7.111	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	3
93.173.29.180	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	2
79.176.56.241	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	2
46.19.86.89	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	2
79.178.28.198	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
95.86.74.212	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluum-ishi.aka.idf.il/changepassword/newpassword	Block	2
46.19.85.95	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.95 (sigalgs DoS Attack)	None	2
62.90.58.17	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
212.179.42.66	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in miluum-ishi.aka.idf.il/generalpetition	Block	2
46.19.85.95	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
80.179.204.224	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
212.179.242.101	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	2
79.182.116.248	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
79.176.48.53	Israel	147.237.0.121		Unknown Parameter ct100\$ContentPlaceHolder1\$fuAddDocsFiles in www.miluum-ishi.aka.idf.il/medicalcommitteerequest	Block	2
46.19.86.59	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.190.114	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 032E449F162C945471BFBC4E03472079EEA68190F89BD64B7ACEAF0F24EF7028BDCFE5AE9F5064C4AEF627EF4804F43C33F4F5B64B404F236FFE4C81279E59ABE8C702C699BFB02C61D03237BEEB0366620C21815C1BC2287E9F9E32993674A242BD1D79E55F11772F396EA45C98AB07552EE8312BDE44B4CF1A6D2C6B2ED1B, Observed 2496E086FB002D37612A5C2660ED37AE5A86830AF36E6EA581FE0D77D95AF087EF263487EE583E3D6BE4C20F3CC0A838D3B331DCFA7F1DACCDE99741211A2F3E12FB6447B294AD4BB25A71961F4DDD62ED0136E9C7654879AFAD3D288565AC381B6570	None	2
84.111.180.87	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.114.105.254	Israel	147.237.0.121		Suspicious Response Code	Block	2
79.183.154.248	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	2
79.178.28.198	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value 65BB5B4589D46A32C61E7E9167FCF19C6E552D307CE34A4AC16ED0E739C2B6AFE7661197A43637A58FB48908D55DC566802D818B6F672378C0C180F1AA1D19D525C0656F6CD9CD0A275034D87DA11290114EEDF37563D073ACA8ADC4E6035BD3793070E3D0E32C0D9708B28238DE71EBBC941DB40FC0E7825B616C99555335AA41524F576C14CA13A9AE8E1FB90B8EFBDBE7D4FD0D8D41CF59B535B2CCACF8BE	None	1
132.68.53.209	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
62.90.220.6	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
37.142.192.38	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
89.139.43.98	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
82.80.95.158	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
212.235.98.139	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
176.228.11.48	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
79.183.145.65	Israel	147.237.0.121		Parameter Type Violation ct100_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
109.253.130.119	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
91.231.193.150	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
31.210.188.17	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
217.132.13.82	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 29FA5D8EF902098DB991B5C8BA0DC57271F622EB05A6369CB0A0638FEE24B2EF86B16A10EBB14F274AF096712B9CC5540E9396C1F8EEC4D878E59C7207AC975A33808262221930933E3BDFF9514BD12C6B1247EE68BD8C1D70237FF6376879983CEB7D29BCB210D19D1F8427F6348921E4A7BD7FEE27AFA03E324492A45EC9A691A797ECCB8886B2E1C5370A5A816A1B30BEB77F6A96E93A3668ADC2945135C9	None	1
85.250.34.30	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value 70B040180072C102343AD43D311880BBADDDA7969773C49CAD7F43F17FD07F345D41629B6203176B0EAC087CF44F9FE1093AE79B921315353489E16ED9FE6028A5C1CAB244651EF1BE3C3DFF1B173676B3C8A747DE0EC33F0BDEC377F2870B760CDCEE5E5369ABCF1B292C310C4337341CE6AB2CE24FF651499E0F2AA4820B334257D85D7CD6A5C133DDF48D043A0B7519D549F05BB84E7CD3080F47AFF970	None	1
80.179.204.224	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 80.179.204.224 (Unknown SSL Session)	None	1
195.189.193.1	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100\$txtNewPass1 in www.miluum-ishi.aka.idf.il/personalsettings	Block	1
147.236.38.173	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
77.125.89.108	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
83.130.100.199	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
213.57.242.172	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
185.120.125.53		147.237.0.121		Suspicious Response Code	Block	1
79.183.145.65	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
79.177.62.226	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
91.231.193.150	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
85.250.34.30	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
80.179.204.224	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
165.72.200.11	Europe	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
79.180.197.150	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
79.176.48.53	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1

01-26-2016 to 01-27-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.160.179.189	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	1
91.227.71.250	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
213.57.253.26	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
84.108.39.118	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
188.120.148.216	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.183.145.65	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
79.177.115.14	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
132.68.53.209	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 132.68.53.209 (Unknown SSL Session)	None	1
91.231.193.150	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.90.99.64	Israel	147.237.0.121		Suspicious Response Code	Block	1
37.26.149.235	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
85.250.34.30	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.35.45	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
91.231.193.150	Israel	147.237.0.121		Distributed Cookie Injection on token: .ASPXAUTH	None	1
217.132.8.231	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1

01-26-2016 to 01-27-2016