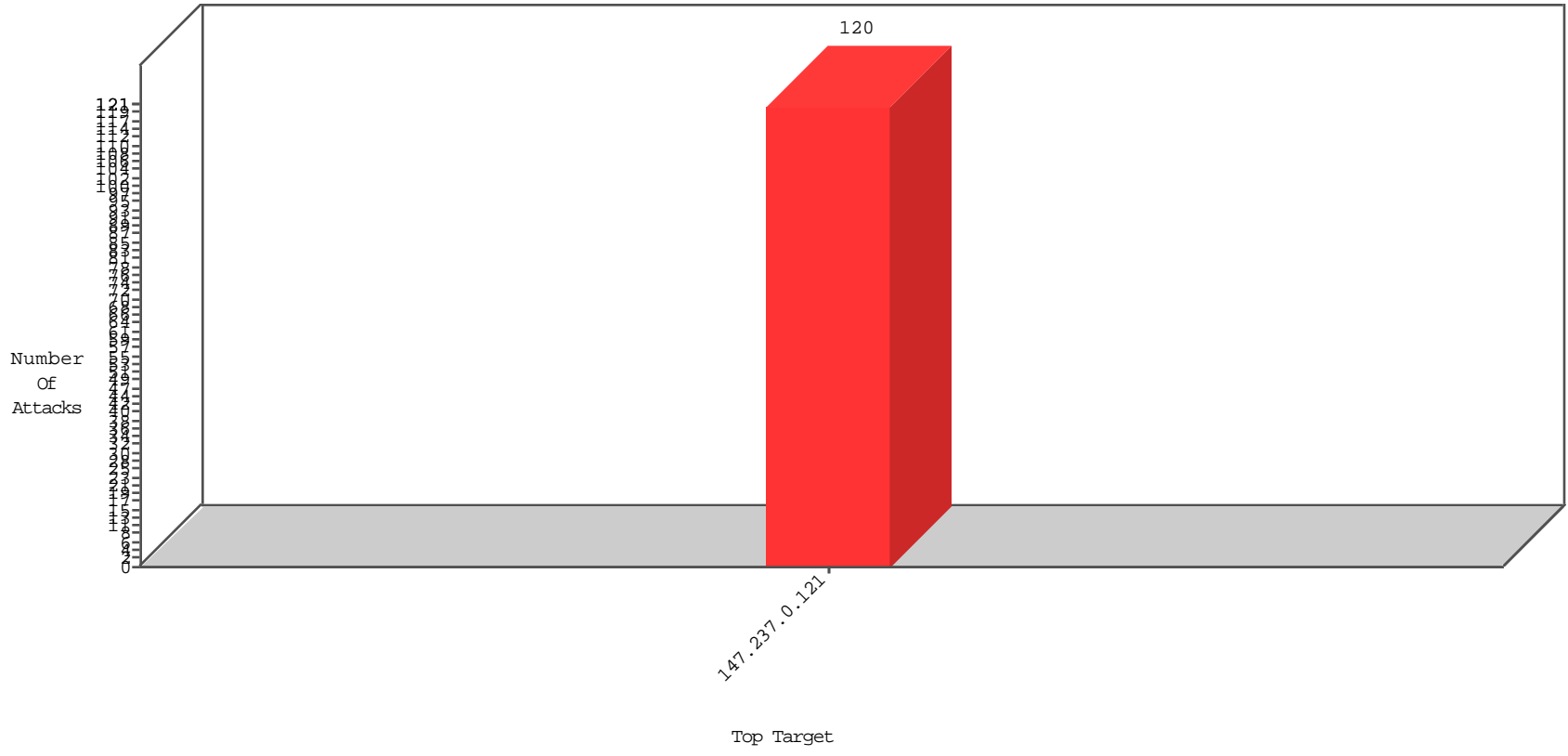


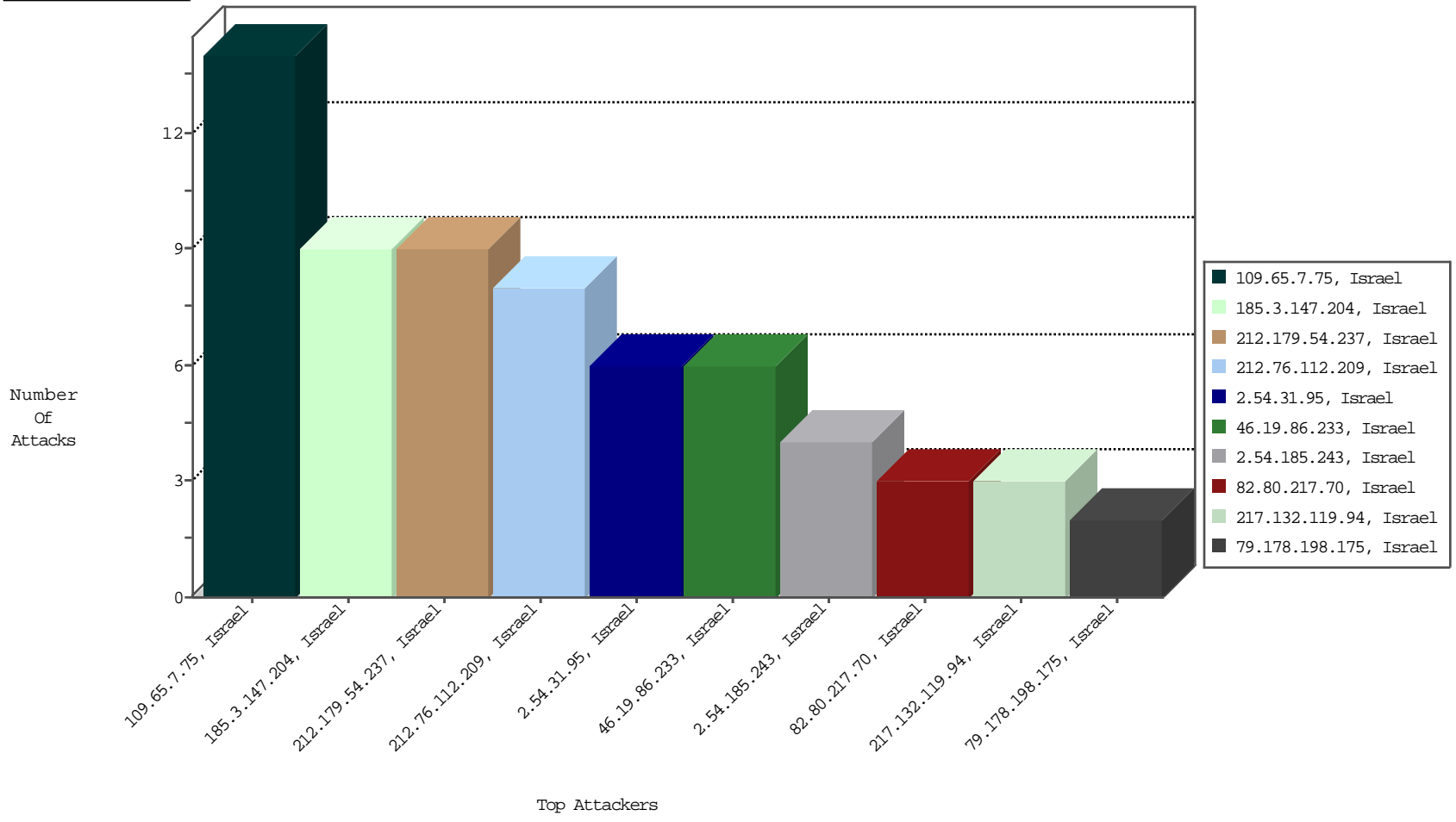
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
109.65.7.75	Israel	147.237.0.121		Block_Udp_All_Nets	drop	EEL-Isreal	14
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	EEL-Isreal	9
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	EEL-Isreal	3

01-31-2016 to 02-01-2016

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
40.114.11.138	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
192.198.151.37	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
218.246.0.97	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1
188.120.148.138	Israel	147.237.0.121		ET SCAN NMAP -sA (2)	1
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
84.109.57.34	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7624
204.93.58.176	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4589
158.116.225.93	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	672
31.154.4.18	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	362
5.22.135.113	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	360
149.78.242.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	338
149.78.25.193	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	327
31.154.4.18	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	324
72.69.224.92	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	296
149.88.69.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	293
46.19.85.177	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	270
149.88.202.196	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	260
149.88.14.55	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	247
31.154.5.110	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	243
77.126.237.67	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
149.50.71.237	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	234
149.88.158.71	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	231
149.78.233.80	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	226
181.50.76.50	Colombia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	193
135.245.224.4	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	189
192.88.162.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	157
85.158.139.227	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	147
149.88.124.247	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	142
149.78.22.81	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	141
149.78.225.6	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	135
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	133
149.78.251.202	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	130
149.78.134.192	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
149.78.250.12	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	123
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	117
167.206.154.30	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	115
46.16.142.100	Cyprus	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	114
134.191.232.93	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	106
149.78.143.185	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
192.146.6.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	94
62.90.95.241	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
149.88.67.21	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	89
13.17.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
178.208.171.114	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
109.64.200.202	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
149.78.8.248	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
149.88.153.235	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
185.32.179.40	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	64
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
149.88.140.142	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
112.185.130.163	Korea, Republic of	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
149.88.104.41	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
167.220.196.79	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
194.69.103.20	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
31.154.150.185	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	52

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.3.147.204	Israel	147.237.0.121		Suspicious Response Code	Block	9
2.54.31.95	Israel	147.237.0.121		Suspicious Response Code	Block	6
46.19.86.233	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	4
2.54.185.243	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	4
46.19.86.233	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	2
5.22.130.248	Israel	147.237.0.121		Unknown Parameter ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/smsverify	Block	2
62.90.99.64	Israel	147.237.0.121		Suspicious Response Code	Block	2
192.198.151.44	Europe	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	2
212.235.96.66	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
79.178.198.175	Israel	147.237.0.121		Suspicious Response Code	Block	2
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	2
37.26.148.244	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.124.21	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
46.117.15.13	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 920542604AE6D29FE09340AB79BD9AD0D2EBD1D8D5CF0021DB664388516A7B3EB7F1DCAEF77 6CCF8B8B815A18DC28721BAA7EED70A978D530BBBE21A8A2F320C1E7E91740CEA018F720498 BD467EA9E61BB380BDF3545D678AF55D56E8F0DCB025D75A04547A063C73BE5C7AB44F652EA 1A195121E439D3C8D5D5026BE4BDE85, Observed B0FD8B429F470627379416D6D91B7FF7C1942A5DC451AA30F20D835AE22F12F7C921980670A D97146E8F1A875CAC4F3FB9F1728E41E5258743132C0A8549491328735069605AAC808174374 F357F9089AA86A77899E041949916F3867D4BEFC2F2FC522	None	1
46.19.86.10	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.235.20.125	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 98059BA08CA79A9EB1180678ADAD3DDEBB1A2ACF18D8F5AFE5AC4D8B02EE7CFA3690FD5FCD EC9AF0CE92FE665356EF54AEAAA9CF3C7F71E53D1158BE9C03D5301C64FE66E8CA2C2C806486 7366AA4F91462AA62F81B618795FF7B2339BCB2F78952926ACF07851461893522DF1CB0FC359 2A4F5292D347A31A4A5266EB22CB9D, Observed AB49A55018B67916E11F47A0A466C0358717A7FE2A075906A13B75313E29C850F581044C946 1F785F0D9526EDD43D00E0D87E3ADB22D98FF93A05904DEF30F16D75355347E6050E9FB4BCD3 491B987225E27C3AD4D5AD057C0B58178EA112FE8E7428D	None	1
132.68.50.72	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
5.102.229.112	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
83.130.113.105	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
2.52.190.204	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
77.127.26.209	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
213.57.106.79	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/lobbygma	Block	1
192.198.151.43	Europe	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
37.46.39.116	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
91.199.69.254	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
79.183.124.21	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtTitle in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
46.19.86.45	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.45 (sigalgs DoS Attack)	None	1
212.235.59.4	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
31.154.163.177	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
84.108.249.169	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPass in www.miluum-ishi.aka.idf.il/login	Block	1
79.176.224.32	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesNames in www.miluum-ishi.aka.idf.il/volunteeringbyage	Block	1
217.132.119.94	Israel	147.237.0.121		Suspicious Response Code	Block	1
37.142.146.195	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
5.102.197.227	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	1
109.67.126.190	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
80.74.97.148	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtTitle	Block	1
62.219.99.130	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
46.19.86.45	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
185.120.125.34		147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
31.168.89.122	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
2.54.56.196	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.215.202	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.19.86.235	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
46.19.85.11	Israel	147.237.0.121		Illegal Parameter Encoding __EVENTVALIDATION in www.miluum-ishi.aka.idf.il/personaldetails	None	1
209.88.196.250	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
5.102.197.227	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
109.160.174.161	Israel	147.237.0.121		Double URL Encoding - parameter: returnUrl in www.miluum-ishi.aka.idf.il/login	Block	1
80.230.25.28	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
77.126.209.51	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/newpassword/	Block	1
46.19.86.112	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
213.8.86.146	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
192.116.215.34	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
91.199.69.254	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1