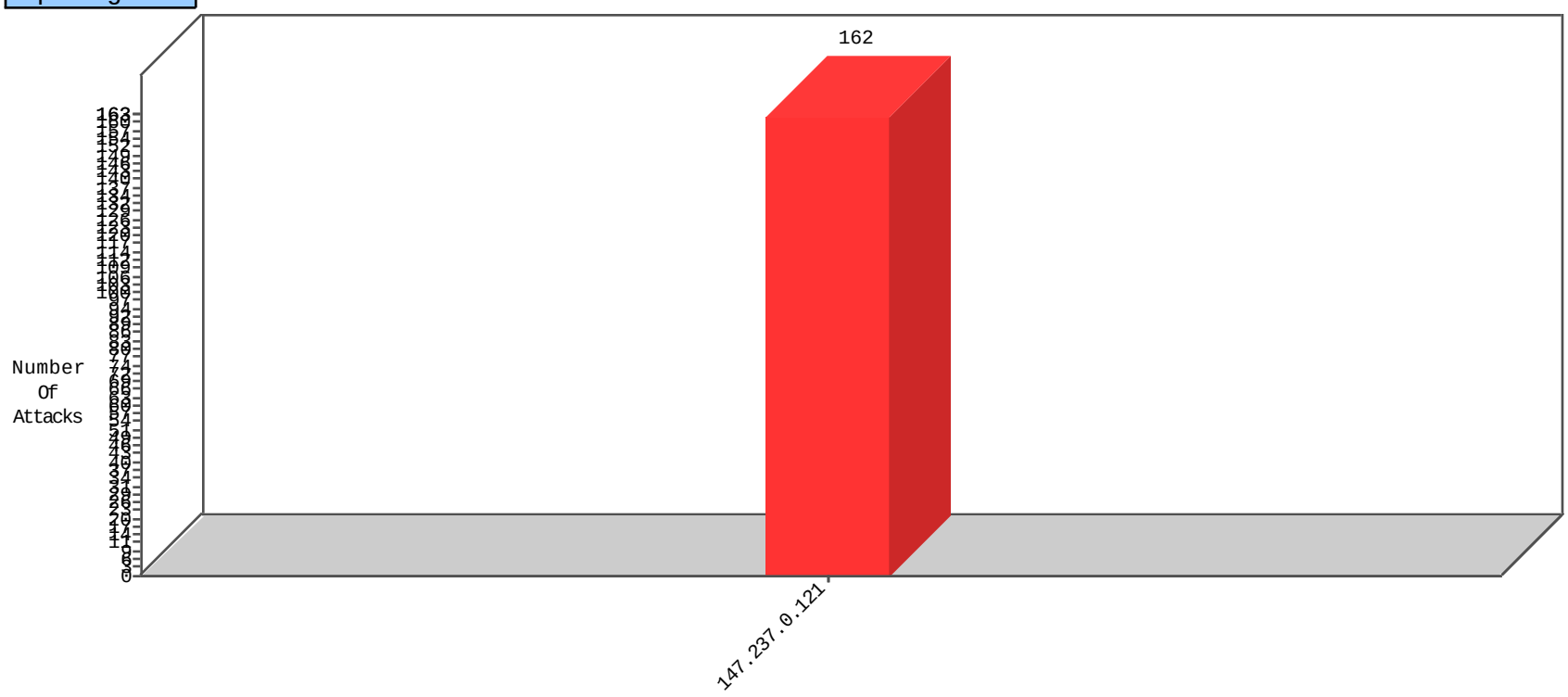
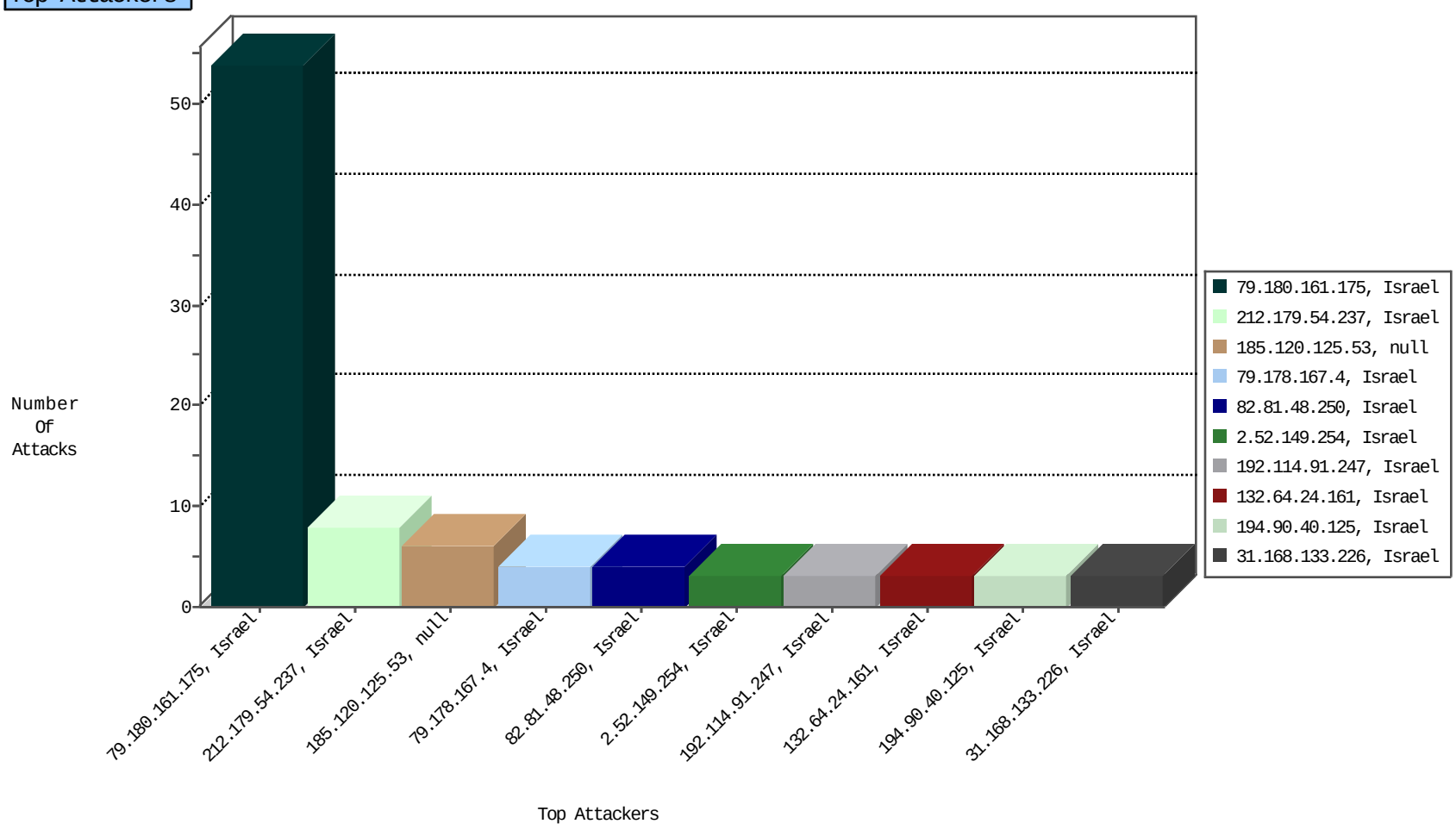
01-19-2016 to 01-20-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-19-2016 to 01-20-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.180.161.175	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	54
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	8
82.81.12.22	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
31.168.133.226	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

01-19-2016 to 01-20-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-19-2016 to 01-20-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
60.209.5.30	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
125.65.165.215	China	147.237.0.121		ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
91.201.236.114	Ukraine	147.237.0.121		ET SCAN NMAP -sS window 1024	1
168.62.238.153	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1

01-19-2016 to 01-20-2016

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	2315
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2210
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1812
149.78.169.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	992
192.232.81.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	450
31.168.89.122	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	342
140.101.20.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	311
149.78.47.5	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	297
210.61.39.253	Taiwan	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	269
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	203
149.78.252.210	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	198
149.88.185.109	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	173
149.78.28.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
149.78.179.151	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	170
149.88.26.211	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	164
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
149.50.73.214	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	157
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	133
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	133
149.78.254.45	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	110
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	88
149.88.7.35	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	84
2.52.34.162	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	74
149.78.42.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
149.88.20.235	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	72
85.158.139.101	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
194.90.119.123	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	62
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
2.52.175.5	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	50
149.78.216.50	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
31.154.145.7	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.64.162.173	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
207.232.41.2	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	32
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
46.19.86.226	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	26
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
2.54.140.9	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
157.55.39.224	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
110.78.187.196	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
199.203.226.21	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	20
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	20
149.78.20.108	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
132.64.83.22	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	19

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.178.167.4	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	4
82.81.48.250	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
46.19.86.27	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	3
194.90.40.125	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	3
132.64.24.161	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	3
46.19.85.109	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.69.35.77	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
2.52.149.254	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
62.90.99.64	Israel	147.237.0.121		Suspicious Response Code	Block	2
192.116.164.166	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
93.172.186.184	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
109.253.141.169	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
217.132.13.19	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
84.108.128.255	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
79.181.218.208	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
212.25.102.57	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
213.57.84.132	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.182.7.30	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value 6DA44E1F7FF6DC869609CFAF222431BDCC9E5BAF6CD4C7770247453B5D66EC6F2174A1977C49DDC3269BA17A7B79611E4BB20F5520AB3D31D7FDC79CEAEC4BC20A5AE03BEA417A5A066BE9047E5A4D2F501D6A12208442914E890AC0CF698DE195FBCA73D8D6BCE937C116D08BED2BF1A8F702387E43039CFA1A47957A594AD2C8E7C940E3B602E6A0E23544711FD553406BE8AD507B102402F09D278D4557A8	None	1
62.0.118.86	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.116.127.113	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
109.253.211.234	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
83.130.106.49	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
212.29.203.226	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 212.29.203.226 (Unknown SSL Session)	None	1
185.120.125.53		147.237.0.121		Suspicious Response Code	Block	1
46.120.77.163	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
2.54.134.104	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.134.104 (sigalgs DoS Attack)	None	1
109.253.130.56	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	1
84.228.236.121	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
213.57.127.2	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00$txtNewPass1 in www.miluim-ishi.aka.idf.il/personalsettings	Block	1
80.246.136.171	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
109.253.219.129	Israel	147.237.0.121		Distributed Parameter Type Violation on miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
2.52.149.254	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
84.94.140.114	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
79.181.102.240	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
212.29.203.226	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
191.240.136.5	Brazil	147.237.0.121		Unauthorized URL Access to 147.237.0.121/vtigercrm/include/style.css	Block	1
46.121.247.2	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
2.54.134.104	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
85.65.111.15	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
80.246.137.97	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.90.174.102	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.73	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
2.54.7.245	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.7.245 (sigalgs DoS Attack)	None	1
94.230.86.234	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/newpassword/forgotpasswor	Block	1
212.68.157.162	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
192.115.67.2	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
62.0.118.86	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 62.0.118.86 (sigalgs DoS Attack)	None	1
46.19.85.82	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	1
109.253.151.37	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
85.159.165.18	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected C0DEDA4021A71A075B7BA9453DEDC9007DED2D2519F48D4325C29F83B60BCB367E3CA990A8BF9CE93639DE27E4776EDCD02E0B0191AC1D4A669C47DB23DC9E22843D87C2624E16E0FC73AA086155C668FFBF3349B46B84567C47B420AADBA0DB28375C863AF1AD4E0FC1B55A2BA817102DB14829E5E717BDC6761A28181397A0, Observed 0631AE83C633328A548DD053B8B7D0F828F82A039CD2A9861A46509F2F368A60A04680FB98D4D6A1497D63DAF5C522F2941A251A18CCEB967487CFDF332B508B3956B4B0AE7E99EB7CC59C6CCF960DAEDE77C61237FC7CBFABD5ABC3324D7C767F72B7	None	1
2.52.133.235	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
79.178.15.248	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
176.13.22.27	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.94	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.7.245	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.66.116.95	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
84.111.136.54	Israel	147.237.0.121		Suspicious Response Code	Block	1