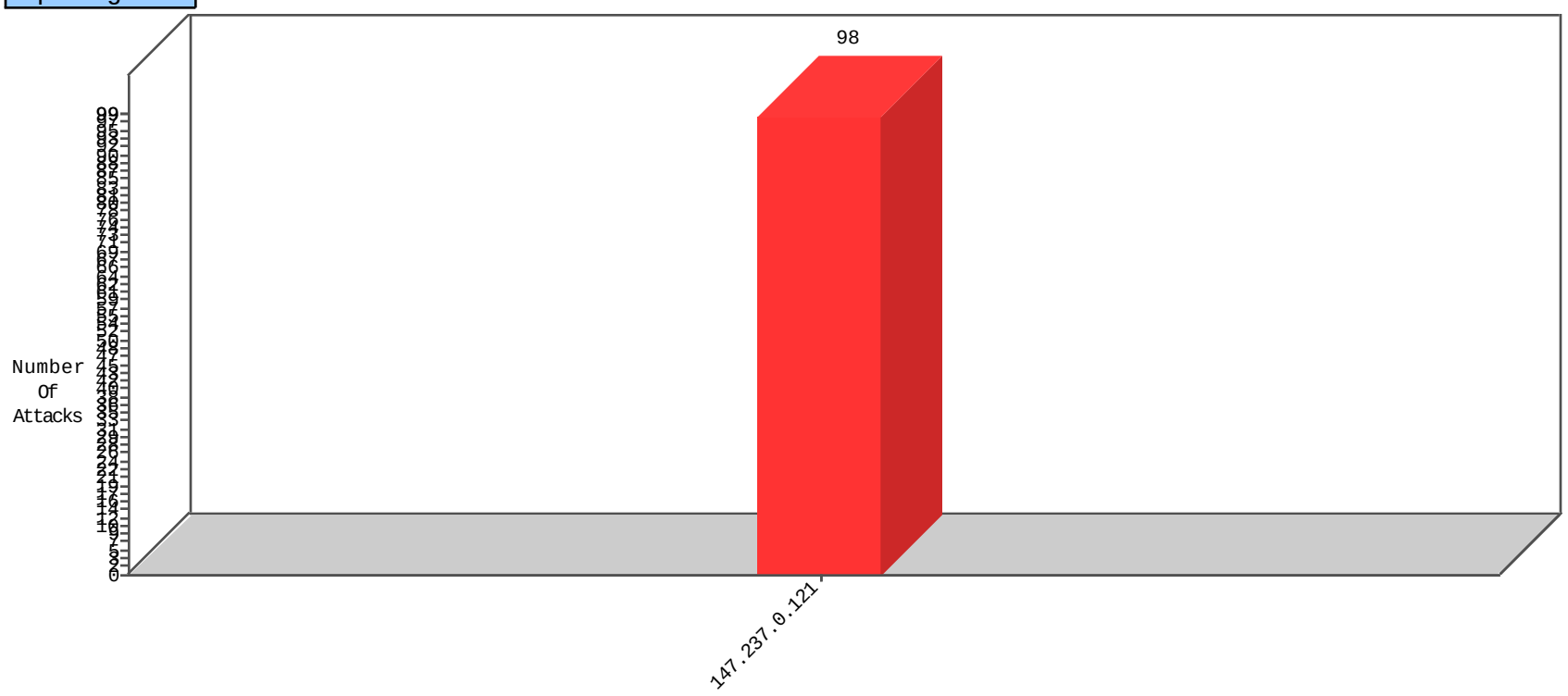
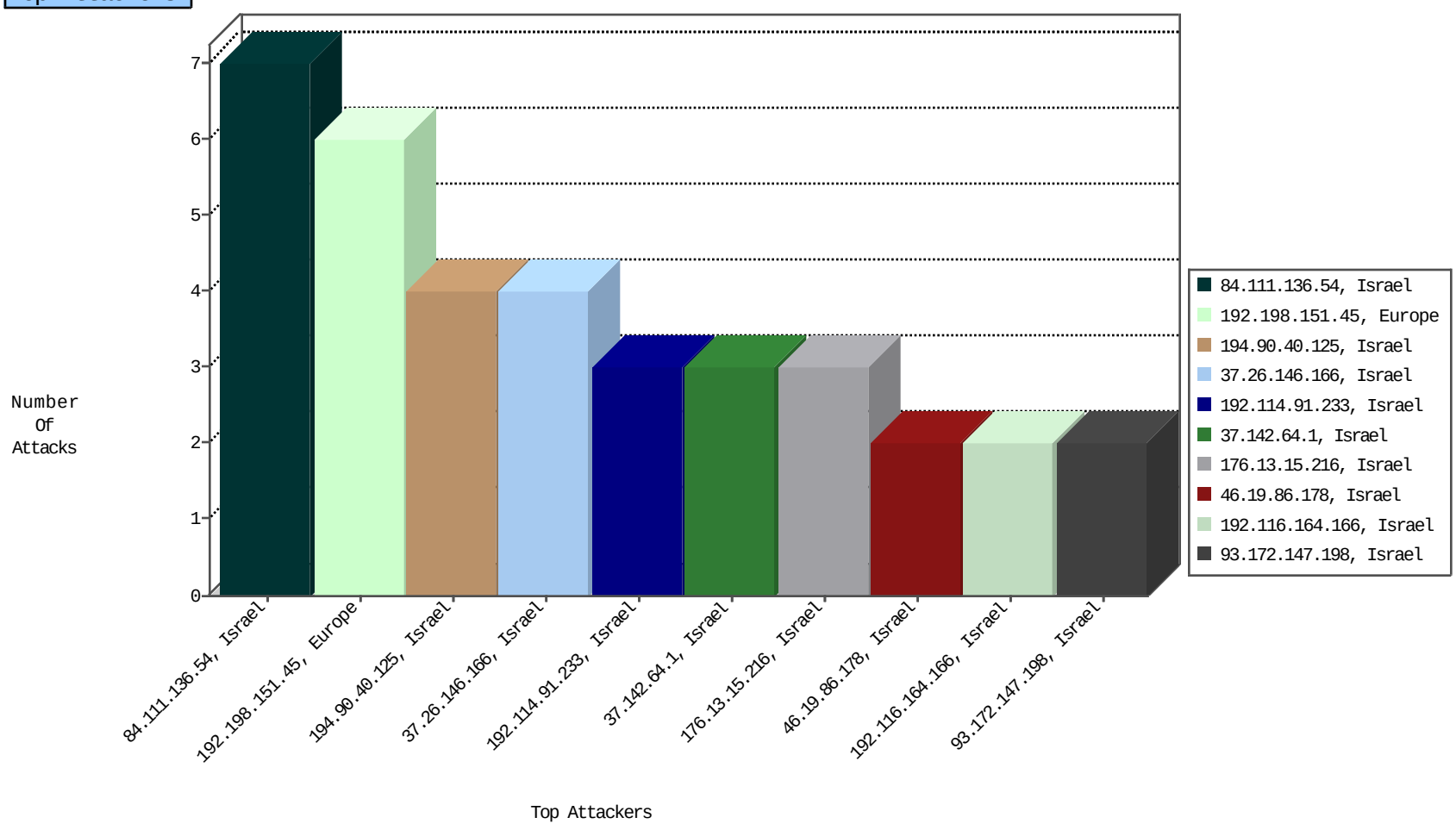
01-17-2016 to 01-18-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-17-2016 to 01-18-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count

01-17-2016 to 01-18-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-17-2016 to 01-18-2016

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)	6
84.109.235.9	Israel	147.237.0.121		ET SCAN NMAP -sA (2)	2
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
168.62.238.153	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
191.240.136.5	Brazil	147.237.0.121		ET SCAN NMAP -sS window 1024	1
194.187.249.70	Europe	147.237.0.121		ET SCAN NMAP -sS window 1024	1
58.16.129.102	China	147.237.0.121		ET SCAN Potential SSH Scan	1
82.78.176.114	Romania	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
183.60.48.25	China	147.237.0.121		ET SCAN Potential SSH Scan	1

01-17-2016 to 01-18-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2640
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2500
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1614
62.219.236.166	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1179
62.168.35.125	Czech Republic	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	440
108.171.128.172	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	404
149.78.169.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	323
62.168.35.67	Czech Republic	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	300
134.191.232.72	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	294
149.88.242.15	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	290
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	253
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	196
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	184
149.78.27.111	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	154
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	152
46.19.86.204	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
84.228.190.194	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	106
149.78.229.33	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
149.88.186.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	98
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	97
54.172.21.120	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
149.78.238.35	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
149.88.158.152	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
149.50.78.93	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
149.78.229.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
138.134.102.16	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
149.88.67.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
8.37.100.38	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
167.220.196.107	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
110.77.249.181	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
73.189.142.102	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
82.81.55.160	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
212.235.27.186	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
82.81.55.160	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
185.32.179.81	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	31
149.78.176.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
81.218.241.25	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	29
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28

01-17-2016 to 01-18-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.111.136.54	Israel	147.237.0.121		Suspicious Response Code	Block	7
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
37.26.146.166	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	3
176.13.15.216	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	3
37.142.64.1	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	3
217.132.60.25	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	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
87.69.140.47	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
5.29.41.56	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
192.114.91.233	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.24	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.253.216.80	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
95.86.112.9	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
37.26.146.166	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
85.64.250.163	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
80.246.137.123	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
185.120.125.8		147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
46.19.86.178	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.142.64.32	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
109.65.80.210	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected A472D630438D28FB4120A344FF4E6941C51D23724E84587D5E8FF6C7153B20A2F33D0D2D4B74AEBA07549B408BCF26880389C1646E12759AD798710E62840EB482098A43EC9F185647D884605A269D6F415DDED9E224112694AF0A4DCDD4F9A230F51222C0F1A70ADE963F3B028FCC589E44061605D71E588657C0233AA727E0, Observed 1AC01D5FD16DD33A7A85E7ABA14082ABD2ACAC1D5F940BDEED697E7731BA1BB33BA8FAD2ECA1B0F3FDE4864105857A5807D255F1549DF3BD1B2F07E8149249BCD0A00EA1C4B081A523B096B655C1198BDCDAE0808A2371F35EBD2BF89FF9DBA6430BF7	None	1
93.172.147.198	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
5.22.135.50	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
213.57.105.37	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 2835875D9383F2FED8BA21002124EA88C170A9DECE5757A1F61327908809E8F0B45BCF5E03012C5817F4826BB48B33E358601E7D2F327EC861E5752B79F35967432C42A686FE1A8B88D31188810B6B74371AFE98DFAC325D1ED04BA59EBC906F5B30F2755833A1D36B24AC5F79DD2E3A8DF50C2A2FA40F92FA2487A63F8C864E, Observed 4C493240EE5A1C54D650E3D21D301BD5E52CAD18348A6100EE6D98A2DC67AFC7D85B1B4C9BE89B250AC553D6BFDE434548E884635F16F05A67059724BA29829D833D2DD302785BC204FA84A74479CD82A3BD54A81E9737FEE45D1D1B3D8E6826ECED9C	None	1
82.80.29.90	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
79.179.15.131	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
176.13.12.218	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
46.19.86.27	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
109.64.96.120	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
80.246.139.171	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	1
212.25.107.145	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
192.114.91.233	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value DD7FBD75B59CEFF033D73E964A2A8ADEC13B497BA4299D01E926AB5CD27DA6461797F39E17A1B80C61C03E7CEDFAF77C13A1BBA44C9C906BC218817DB38F6B78102DCD261A7102B5CA83CB6A6CCD5B32A86E416D300DB7D182117C400213740994A2A6BA071BB6F44619A9309CAE3416CC95D56D73595B732238CA9101356FE2233EDD3B2991EF068A9EABC33837C4BB99F85CC1633C46EEC8EEA5E1AF0F13B8	None	1
77.127.135.204	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 02222693BC434FC06B1CB2B25A1923A1306D0B96A9F30B202CB6394BB4D7B3C54467D0BB1EA9ADB88C11AA0AB7401EE180BC509B9675792638CE580B5F5C8D392373814C437378AFE335DCE1B6755A9A340D6116290082CD5DC0400171B34723AC144838ACE5D2D5F1CD5CB9A74D89FA357B8230F12E03A73F107C3DEFE96EA0, Observed 9311CE1DDB5314DC97AF62FC11FD2957FBB8918CBF363EB94C8BDC041BEBBF73E9702FA2A308AD61F3BB30DC6576D92411DFDB1447A0494E37B6EA1503E52634BE93AF1657D44293E58A85240700FC751C0209EEEC02FCC2279860621230D35E54E123	None	1
37.142.131.36	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
109.67.140.76	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.147.198	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
217.132.32.217	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
84.110.211.102	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
79.180.122.153	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
192.116.213.210	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
46.19.86.108	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.26.148.193	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
109.64.105.129	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.64.105.129 (Unknown SSL Session)	None	1
89.138.3.115	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
2.52.39.243	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
80.246.140.251	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	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
79.177.199.25	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
46.19.85.90	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
109.253.151.44	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
94.230.86.220	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
31.210.188.117	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
217.132.35.94	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
79.183.190.75	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1

01-17-2016 to 01-18-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
194.90.40.125	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
185.27.105.76	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
46.19.86.178	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.178 (sigalgs DoS Attack)	None	1
109.64.105.129	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
92.61.225.10	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
2.54.190.28	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
212.29.203.226	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
81.218.97.45	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
192.114.182.2	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
79.178.15.248	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1

01-17-2016 to 01-18-2016