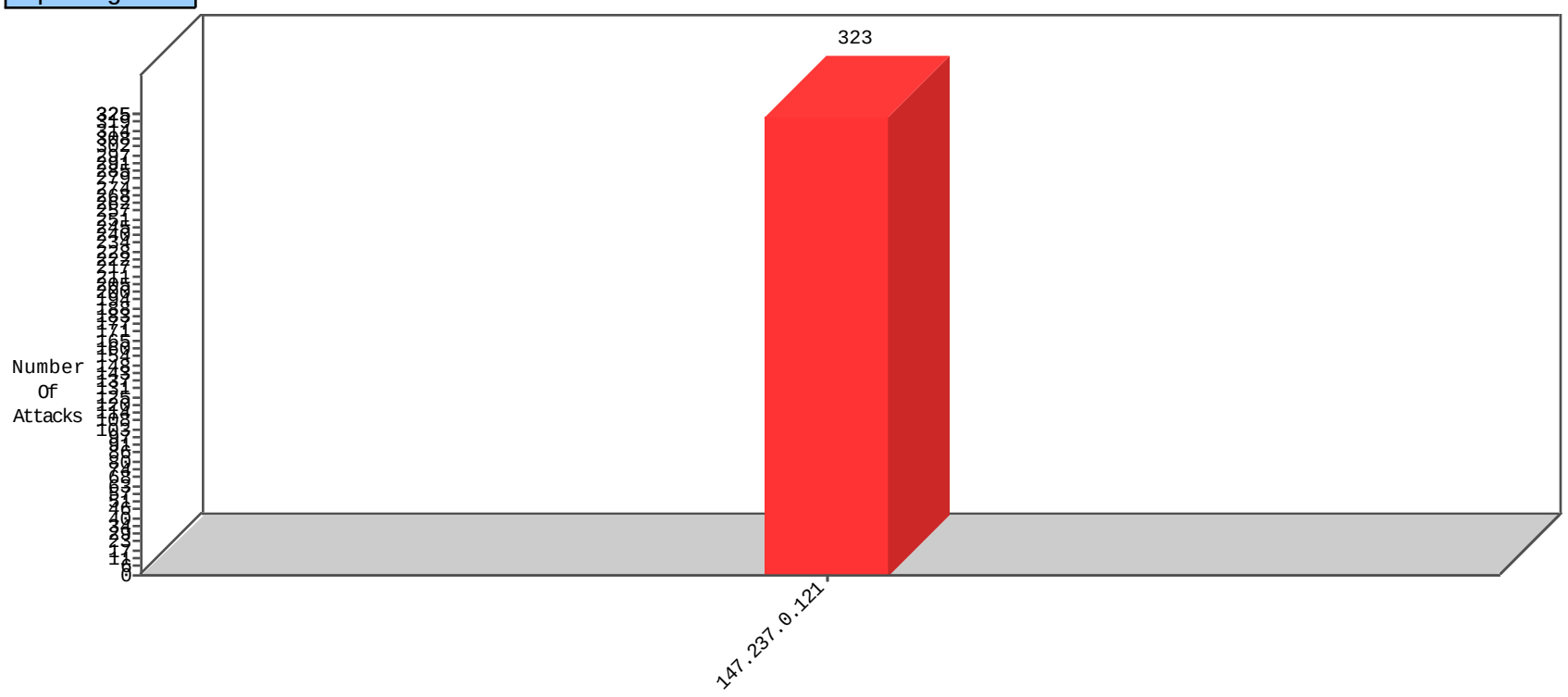
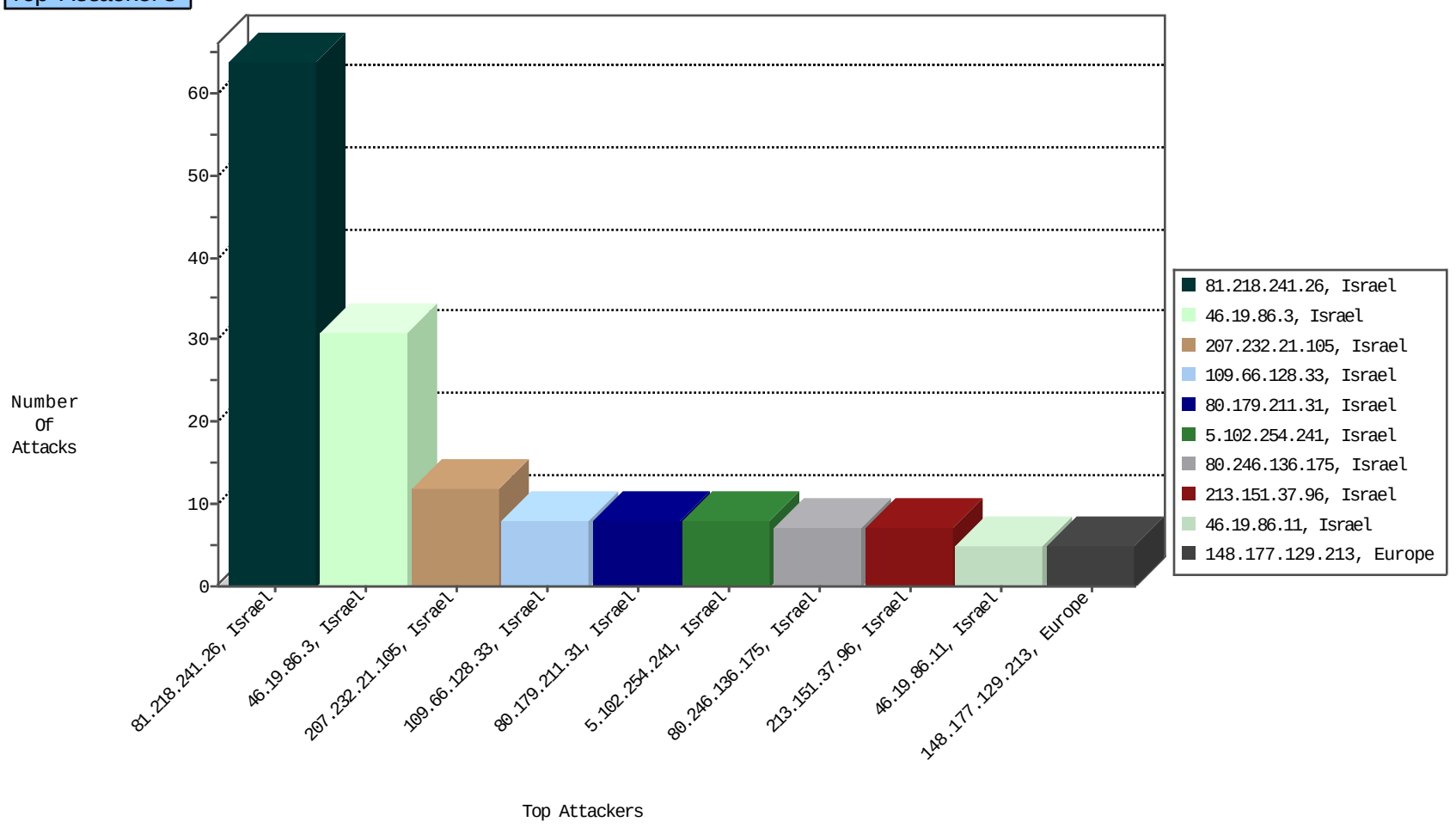
01-12-2016 to 01-13-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-12-2016 to 01-13-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
81.218.241.26	Israel	147.237.0.121		Anomaly-TLS-renegotiation-Cli	dest-reset	BBL-Israel	64
46.19.86.3	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	31
46.19.86.115	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	5
31.168.225.146	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
222.186.56.42	China	147.237.0.121		Frk_Under_Attack_Con_Tcp	drop	BBL-Frankfurt	2

01-12-2016 to 01-13-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-12-2016 to 01-13-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
89.248.172.173	Netherlands	147.237.0.121		ET SCAN Potential SSH Scan	1
164.39.11.198	United Kingdom	147.237.0.121		ET SCAN NMAP -sS window 1024	1
104.207.152.230	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
180.97.106.37	China	147.237.0.121		ET SCAN Potential SSH Scan	1

01-12-2016 to 01-13-2016

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	2147
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1994
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1426
85.115.54.202	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	947
149.78.226.247	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	364
149.88.7.123	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	334
84.94.198.136	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
149.78.39.20	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	324
157.55.39.156	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	296
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	265
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	246
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	242
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	237
149.88.149.169	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	216
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	164
149.88.238.126	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	156
200.91.148.178	Costa Rica	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	145
85.158.139.227	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	145
2.54.58.22	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
46.19.86.207	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.174.8	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	133
149.88.58.39	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	128
54.243.190.43	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	107
149.88.242.15	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
167.220.196.166	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
149.88.31.7	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	75
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
94.230.86.192	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	72
94.230.86.192	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	72
149.88.76.5	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	58
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
46.19.86.3	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
149.88.13.144	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
49.224.199.66	New Zealand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
153.92.126.19	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
194.114.146.227	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	37
207.46.13.14	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
192.114.23.209	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
2.52.55.97	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
192.114.23.209	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
149.78.247.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
79.183.191.178	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	29
5.29.183.191	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	25
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
40.77.167.62	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
81.218.241.26	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25

01-12-2016 to 01-13-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
80.179.211.31	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	8
207.232.21.105	Israel	147.237.0.121		Distributed Double URL Encoding	Block	7
109.66.128.33	Israel	147.237.0.121		Suspicious Response Code	Block	6
109.253.202.108	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	5
31.168.13.78	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass2 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	5
212.199.123.251	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	4
207.232.21.105	Israel	147.237.0.121		Unknown Parameter virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	4
46.19.86.11	Israel	147.237.0.121		Distributed Double URL Encoding	Block	4
46.19.86.0	Israel	147.237.0.121		Distributed Double URL Encoding	Block	3
109.253.199.179	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	3
31.168.178.121	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	3
213.8.247.58	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	3
79.178.97.61	Israel	147.237.0.121		Unauthorized HTTP Method	Block	3
95.86.95.186	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	3
109.253.141.104	Israel	147.237.0.121		Distributed Double URL Encoding	Block	2
109.64.103.124	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
82.80.29.90	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/loging	Block	2
80.246.136.8	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
5.28.137.148	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
109.253.201.176	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
83.130.115.195	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
31.210.183.144	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
213.151.37.96	Israel	147.237.0.121		Suspicious Response Code	Block	1
2.54.144.157	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
80.246.136.220	Israel	147.237.0.121		Distributed Double URL Encoding	Block	1
79.180.218.117	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
176.13.19.177	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.121.123.18	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.11	Israel	147.237.0.121		Distributed Unknown Parameter on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
85.64.7.190	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
81.218.156.84	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
31.168.11.194	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
212.25.102.57	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
2.54.11.34	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
192.114.105.254	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
77.125.240.47	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
46.31.103.99	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.108.217.240	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.108.217.240 (Unknown SSL Session)	None	1
46.19.85.198	Israel	147.237.0.121		Distributed Unknown Parameter on www.miluim-ishi.aka.idf.il/cellularreference parameter cellularType	Block	1
217.132.36.187	Israel	147.237.0.121		Distributed Double URL Encoding	Block	1
5.22.129.64	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
207.232.21.105	Israel	147.237.0.121		Double URL Encoding - parameter: virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
80.246.138.208	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
79.182.242.132	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
185.3.146.242	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
109.253.141.104	Israel	147.237.0.121		Unknown Parameter cellularType in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
46.121.193.145	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
46.19.86.121	Israel	147.237.0.121		Suspicious Response Code	Block	1
87.68.241.236	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 7EABCDD63702E11E36CA9386C4790EAEF20103493D303CD506238C5C2DDD24A5D84F00514BE1478986119CC562AC1BE5E3AA1108D868BF7C99C582E51DCE1A590EBF3952397697DDA46BE0B5E38363D021C3CF078B53B8E2384EC1E32E336FEC2AD8CBE5A7D0D0EDACB65EE58D3BA7A5FF1FFE84DFE17C65882936357F4FE367, Observed 8EA7B35B53C531C271C0AD99B597EF54A62EF8382E2B28BC3DA6EBC619167219240103C4B0C2929C9FA5E4773DB3313E02588827237194FDA8B1872AA991B38DFD8A80C3F1D562F51EF6E360466AFA5C9D1E963FB9DD87436DCCB7729ED2BE798E9991	None	1
2.54.36.13	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.114.173.74	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
79.176.173.24	Israel	147.237.0.121		Distributed Double URL Encoding	Block	1
109.253.213.67	Israel	147.237.0.121		Distributed Double URL Encoding	Block	1
46.121.77.183	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.217.240	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
80.246.139.82	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
79.183.230.50	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
185.3.147.50	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
62.219.86.253	Israel	147.237.0.121		Unknown Parameter returnurl in miluim-ishi.aka.idf.il/login	Block	1
46.19.86.146	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
95.86.87.133	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
82.166.198.101	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
2.54.144.157	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.144.157 (sigalgs DoS Attack)	None	1
192.118.30.102	Israel	147.237.0.121		Unknown Parameter **** in www.miluim-ishi.aka.idf.il/login	Block	1
80.246.136.175	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
132.72.9.228	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
109.160.148.147	Israel	147.237.0.121		Unknown Parameter tzav in www.miluim-ishi.aka.idf.il/login	Block	1
46.121.111.241	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
84.109.0.24	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
81.218.71.132	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
5.102.254.174	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1

01-12-2016 to 01-13-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.25.102.57	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 212.25.102.57 (Open Mode)	None	1
80.179.200.203	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
192.114.91.245	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
62.219.86.253	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	1
46.31.103.99	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.31.103.99 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1

01-12-2016 to 01-13-2016