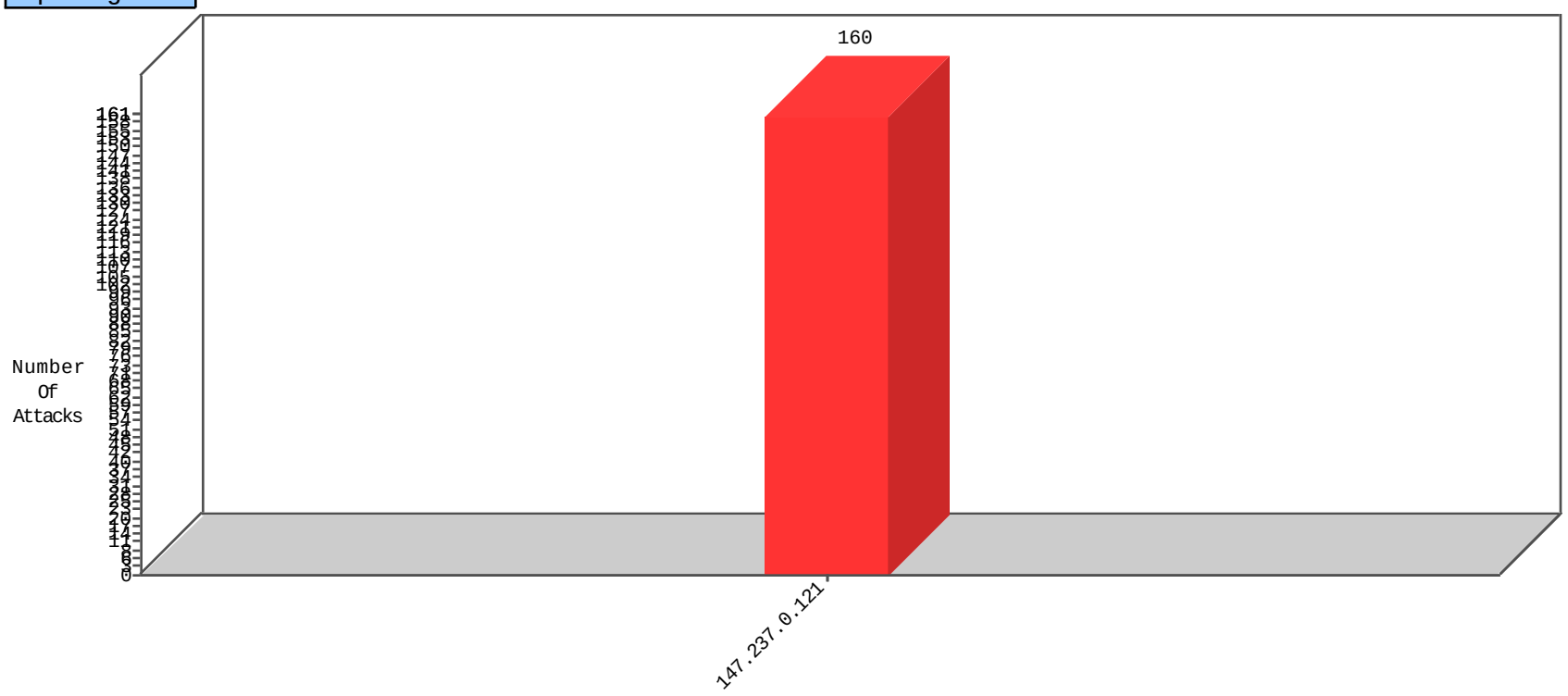
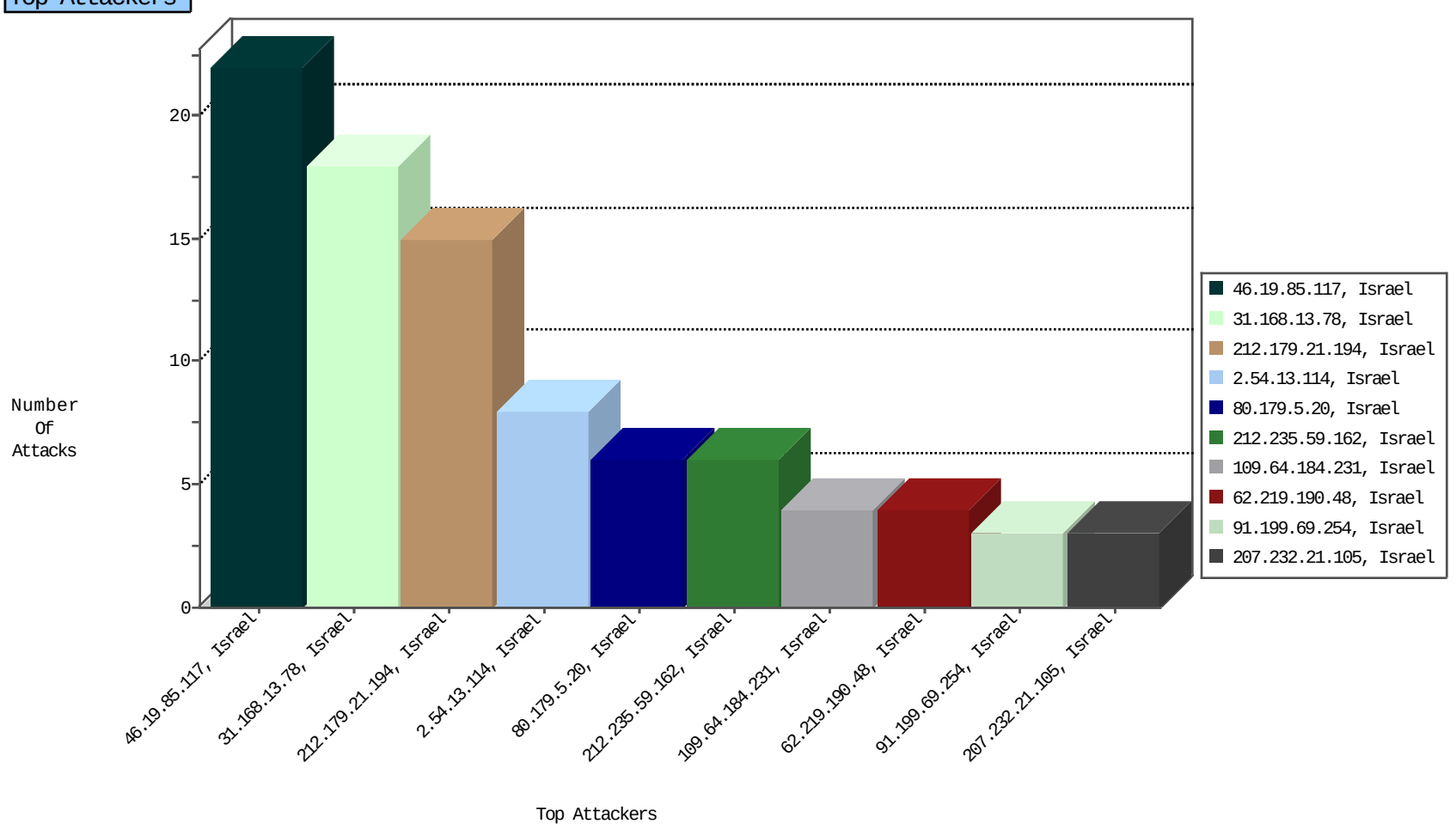
01-07-2016 to 01-08-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-07-2016 to 01-08-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
46.19.85.117	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	22
2.54.13.114	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	8
31.168.133.226	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
79.179.137.13	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

01-07-2016 to 01-08-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-07-2016 to 01-08-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
94.102.48.195	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
201.160.77.135	Mexico	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.219.164.58	Mexico	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

01-07-2016 to 01-08-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
213.57.252.126	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2888
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2360
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1745
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1608
149.78.29.41	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	340
68.180.229.110	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	309
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	257
209.88.192.97	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	213
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	201
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	190
149.88.52.63	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	173
15.90.166.11	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
149.78.27.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	158
2.54.60.99	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
217.132.6.84	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.182.138.234	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	133
176.228.6.214	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	128
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	111
2.54.63.215	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
66.249.93.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
68.180.228.168	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
80.246.139.152	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
149.88.132.190	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
66.249.81.254	United States	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	69
149.88.192.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
15.90.162.12	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
80.246.139.239	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	56
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
80.246.139.239	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	42
66.249.69.175	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
2.52.31.165	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	40
2.52.31.165	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	40
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
2.54.13.114	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.180.215	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
213.8.204.7	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
24.77.44.67	Canada	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
149.78.200.81	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.78.39.184	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
2.64.84.239	Sweden	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
80.246.139.239	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
66.249.69.90	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24

01-07-2016 to 01-08-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	9
80.179.5.20	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	6
31.168.13.78	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddBoardExamsPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	6
31.168.13.78	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	6
212.235.59.162	Israel	147.237.0.121		Unauthorized HTTP Method	Block	5
212.179.21.194	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	5
31.168.13.78	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	4
62.219.190.48	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	4
109.64.184.231	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	4
79.182.227.202	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	3
193.34.56.101	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
109.253.196.84	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.168.13.78	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 87B4A5F9B59822BC7E2D92B796FE193BFD7D2243484D92CB0AC96647E4D7D2716D28DFD9EDBD BF53E705FDE405AB9BCF39479C90237C8F3EE78E9763F4CF4421913FF299C6233230D9F817F5F7E 85D576B5F4BA4942F1848BAF7368D3D3CE89A48F58F7B20C8836130BEC09EAA55E66B39E38C32 0DA73A230637433A571402E7, Observed 3D5F574083908CBA049E1ACF0C5E21E021F24876DD59DEBE9A2596BFDFC47E2755D5BA797566B DBAE8BEB61CC35AE21DC20684AD73443CE52DFF172AF157E7FDC520DFD97A34BA532CE112A7 034DD86EE517B5F7AE600233730F7C59C8EB77A9344137	None	2
82.80.216.12	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	2
138.134.102.16	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	2
212.199.0.69	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.172.242.111	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.232.21.105	Israel	147.237.0.121		Multiple Unauthorized URL Access from 207.232.21.105	Block	2
37.26.148.181	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	2
84.111.225.35	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
212.179.21.194	Israel	147.237.0.121		Suspicious Response Code	Block	1
82.80.192.100	Israel	147.237.0.121		Distributed Too Many of the Same Response Code (404)	Block	1
46.120.178.251	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.120.178.251 (Open Mode)	None	1
192.198.151.45	Europe	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
185.3.147.246	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	1
46.19.85.204	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.204 (sigalgs DoS Attack)	None	1
91.199.69.254	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	1
84.95.83.134	Israel	147.237.0.121		Multiple Double URL Encoding from 84.95.83.134	Block	1
2.54.61.51	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.235.59.162	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	1
207.232.21.105	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/cellularrefernce	Block	1
185.86.40.1		147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1325-he	Block	1
46.116.68.61	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
37.46.39.78	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
87.68.80.139	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.120.178.251	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
185.6.64.114	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.19.85.204	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
31.168.195.105	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
93.172.242.111	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.109.136.181	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.109.136.181 (sigalgs DoS Attack)	None	1
2.54.147.49	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value BD61DD66F56DC1854C4A25542850F703EDE2F20DEFB7008C5443D0AF5F632342BA4F6406576D 5C9165A5546600ABF851E76AAA2924BBC4B968C71139DB6B9CBB16E2589F8ACFB5A9AB9991D 54692540E2C24AD630EB4184CFE6215872C9B9F9A2B7A5316B90E33C6B9E3A49E3310F2B8E15A FF0BBB706D639A3A7E4879C1767B95A0FFF206E01BF306D1DF2DD6F7EE40D12D4057401B7223F4 F4C58037FEB012	None	1
212.25.105.125	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.116.71.220	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.116.71.220 (Open Mode)	None	1
185.127.10.35		147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	1
46.19.85.72	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.72 (sigalgs DoS Attack)	None	1
91.199.69.254	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 32824DEBE69198ADE572882C35FDB59FE6C04F811376C806456358F1BCEFFFECDAA554ACD3434 E3488CBC7EDC65AF75B25D0A40D44AA969654543E561B7D1E02733C41F520A149660B27A17FA 3DF970392B4E8DD8D1B30948CCAEA9572B6749BF0585F7982F8B7AE3BEB1B3C55D848A4A7120 A55C6CB1772A5CD3F6037282064, Observed 12B7F4357F938EA7EB215AB00C7433A5AC215BFABF53A141B66AE4C1624E7712FAE587B473F1B E5F08F954A18A81A1287BBC3ACCDA0F25ADA9E4041EFED4B48BD77F93D13F2F693852E46C1F64 B3F84DBE2C7ABF1FA5E6CE7E18AD21611AF18A7FB93E	None	1
83.130.101.230	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
199.203.215.1	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	1
185.32.179.83	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
46.19.86.22	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
31.210.188.13	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
84.109.136.181	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.147.49	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.147.49 (sigalgs DoS Attack)	None	1
212.235.98.139	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
81.199.120.253	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.116.71.220	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
192.118.78.57	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/rules.abe	Block	1

01-07-2016 to 01-08-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
176.13.5.38	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.85.72	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
91.199.69.254	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	1
212.235.22.191	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	1
84.95.83.134	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
79.178.37.31	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
185.86.40.1		147.237.0.121		Multiple Unauthorized URL Access from 185.86.40.1	Block	1
46.19.86.199	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
2.54.147.49	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
213.57.158.172	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-07-2016 to 01-08-2016