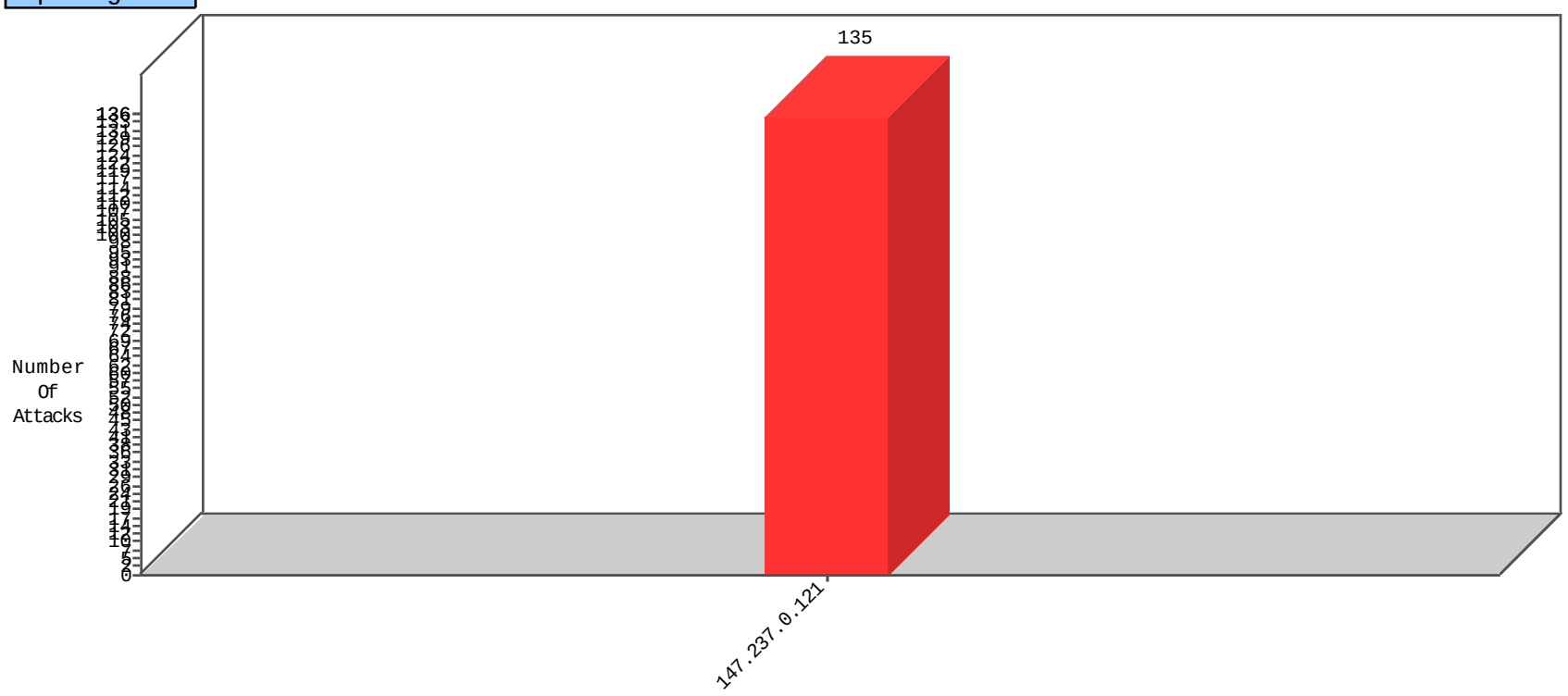
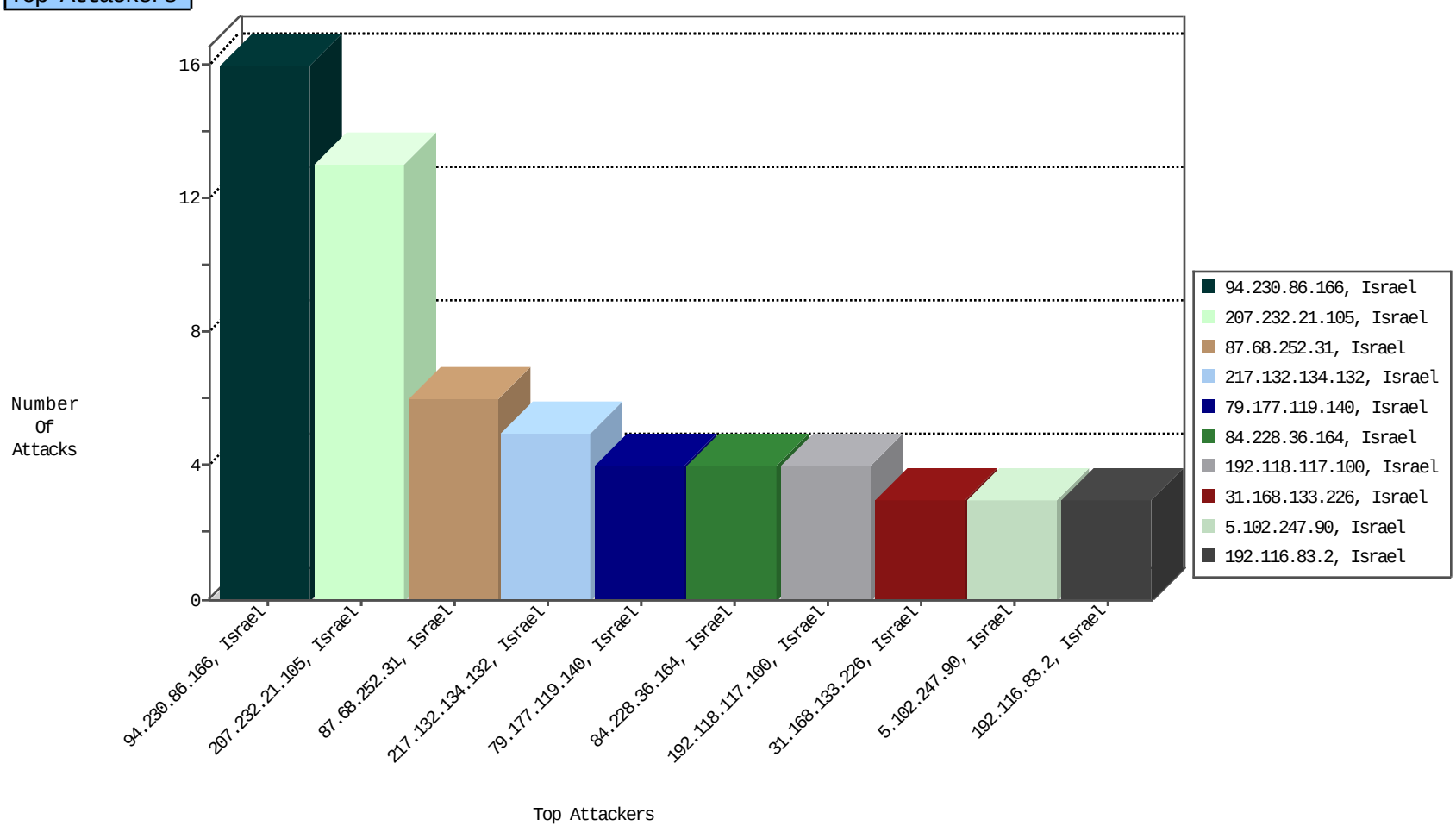
01-03-2016 to 01-04-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-03-2016 to 01-04-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
31.168.133.226	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
81.218.146.238	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

01-03-2016 to 01-04-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-03-2016 to 01-04-2016

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)	3
192.198.151.36	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
188.120.135.12	Israel	147.237.0.121		GPL SCAN nmap TCP	1
173.65.3.44	United States	147.237.0.121		ET SCAN Potential SSH Scan	1

01-03-2016 to 01-04-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3096
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3011
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2627
149.88.106.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	400
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	281
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	259
52.30.171.229	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	226
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	215
149.78.40.110	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	191
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	175
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	158
2.52.182.84	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
5.102.254.209	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
192.115.177.202	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	123
149.88.186.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.224.18	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	84
149.78.105.209	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
149.78.47.118	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
207.232.21.105	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	47
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
213.8.204.7	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
40.77.167.67	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
157.55.39.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
66.102.9.61	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
5.102.254.194	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	32
109.64.16.175	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	29
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.249.93.214	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
81.218.241.25	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	26
192.118.117.100	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	26
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.69.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
213.47.241.66	Austria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
198.15.118.148	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
157.55.39.147	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.74.81	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
185.32.113.34	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	17
82.81.16.166	Israel	147.237.0.121		Bad TCP sequence		monitor	16
212.150.244.200	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
173.245.115.76	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
207.232.21.105	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	13
66.249.69.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
66.249.93.211	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12

01-03-2016 to 01-04-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
94.230.86.166	Israel	147.237.0.121		Suspicious Response Code	Block	16
84.228.36.164	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	4
192.118.117.100	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/form3010	Block	4
87.68.252.31	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	3
79.177.119.140	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	3
192.116.83.2	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	3
5.29.56.179	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/â€?â€Ž	Block	3
207.232.21.105	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	3
5.102.247.90	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	3
217.132.134.132	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	3
207.232.21.105	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
46.19.86.41	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
212.143.110.33	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/form3010	Block	2
207.232.21.105	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/form3010	Block	2
80.179.114.3	Israel	147.237.0.121		Distributed Unauthorized HTTP Method	Block	2
95.86.115.42	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
31.168.13.78	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/form3010	Block	2
217.132.134.132	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
207.232.21.105	Israel	147.237.0.121		Unauthorized URL Access to miluim-ishi.aka.idf.il/form3010	Block	2
109.66.169.242	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
87.68.252.31	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.232.21.105	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtVitur in www.miluim-ishi.aka.idf.il/leaveinunit	Block	2
199.203.68.10	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/form3010	Block	2
89.139.132.107	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/form3010	Block	2
109.253.213.205	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.183.139	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
89.138.46.1	Israel	147.237.0.121		Parameter Type Violation isCharig in www.miluim-ishi.aka.idf.il/ajax/order/displayconfirmmessage.aspx	Block	2
84.109.113.204	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
192.198.151.43	Europe	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
79.177.119.140	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 9DEB413D606CA5BB9D86C7BCFDE8F39B32818E7077F9951B9572E9DBA040D19710688530EA7CC915894371C1789C279759F8FD3E775C7CC88CC5CA163C55653F4B7BC5FE993325BE5F09E66C7F3A1391EE0B1005E356F8C054B1BC50AC7248DA400947CC57CFC5E02D832F4B87B94BA8B8709EF2E4696897404F6539E3A30C3F, Observed E914FB873B40C4FECEC2E0A26BED4BEE9D03ECC9DF7E9CB7F178BC865CC6D69A0C1B981E8DE0FB5D4B9A87902716D8C442B76056ED4446666B2B18CB79DD36A6B8FF6AAB1807039E293D0483977B76D8562A3C179C6A85C63CF51E1DC8A1C9187925BB	None	1
128.139.23.203	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
5.28.128.53	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
89.138.84.199	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
85.64.66.220	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
77.125.141.79	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
185.32.113.34	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
2.54.34.17	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
194.90.15.61	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
62.0.113.48	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
176.13.1.188	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
89.138.84.199	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
5.28.137.148	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
213.8.204.14	Israel	147.237.0.121		Parameter Type Violation __EVENTVALIDATION in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
87.68.34.57	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/volunteeringbyage	Block	1
207.232.21.105	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
81.218.144.209	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
77.126.100.81	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
37.142.150.32	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
2.54.162.70	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.188.16	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
79.179.129.82	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
62.90.151.88	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
176.13.16.83	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/form3010	Block	1
2.52.31.169	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
213.57.92.166	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
87.68.69.145	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 15EE141CC8524CACCD33D4B4A9A0D1CDBA8A81176FE05C6A91A00F49848D733B2C86ACC912BD575C529AED917AB6C29671160F07733FD7EFE6DE0022D991402ABDFD107008FDE69A18257A99C2A4F67A8779A315977D348D9E39BA8F8550C1ABFA664B7AF1968A6F65F9B7D077AE096CFA806A1CBCC2870F8567663D24C0F4AF, Observed 2B29823227E71E030DA7DEB6262316E9B9ACBA8EA217BFC8C404E2D8174481396A3A1BA9FC071111223862F4D8E3D9132D38693DBF3DF775122D7AD3088AC874230340D6E9520257A8458590D69C2E5C8F1BDD31E7E9294A051B1E64A2F04B6CB2EA1E	None	1

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
82.80.144.70	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/newpassword/	Block	1
79.177.81.117	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.85.173	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
84.229.129.177	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/form3010	Block	1
212.76.117.1	Israel	147.237.0.121		Parameter Type Violation isCharig in www.miluim-ishi.aka.idf.il/ajax/order/displayconfirmmessage.aspx	Block	1
207.232.21.105	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 0B3F39612DEE96D94CDFB07E7692228A8707ECF96003B1D2006301F1F8B33DBA794BD187BCB57CA24A50F47E843BA1DC75B3DE9BD90C498E4820FCB957D87AB50F3C5770943AECDF5DCAD7F0559C845C28DB56E82879AD4268531D24C258EA9A836B018E594ACC6C09A617A8A8ECC9A55BB3895CCA6282A6C2EF29364947C3ED, Observed 346CE736810B90A7BE53C1E3C09B5A61F32B759477AAB8BA9FFF55125F41E5150C778F3E4D8366A35FC781457ED1B1A3C096BA5D8F8DD48715BD78A70925B0E957B79E5A8F3AD26EA7B4612C35FB3A7AA23E31A615F376C4D0A336662F1997F8701699	None	1
79.183.212.250	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
77.125.141.79	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
185.3.147.156	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
2.54.11.113	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.252.31	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value 05F8CDAD973A26D4408406A32101BE15F6D80BA8162219CD8C0F7EED81C176D4362745A88351E1FE88BBFC57A3271F38AEC3297455A0D892D643850F79042D1EC08F9DCD88B219F85DF5BAC76E952562FF19A7939E554AEE587D17074F5B315349D4746FFCCE7BF4669B450C412E900BFC9AA08E567BC2E4C6876A4A7F9810FDF3868A03A2486DB4FAB0346DFB3B44C55EEA1211295EBB249819328D4CD2843E	None	1