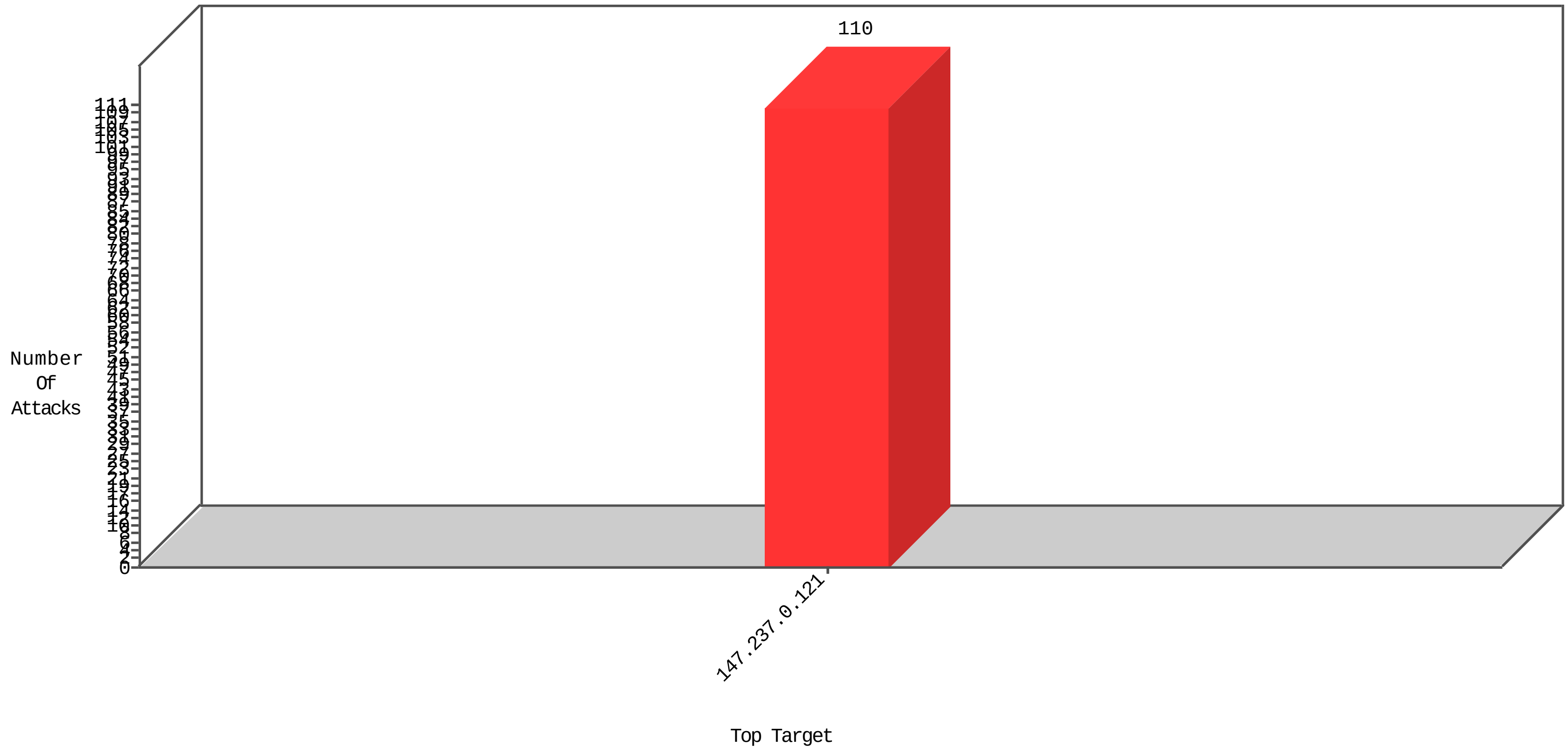
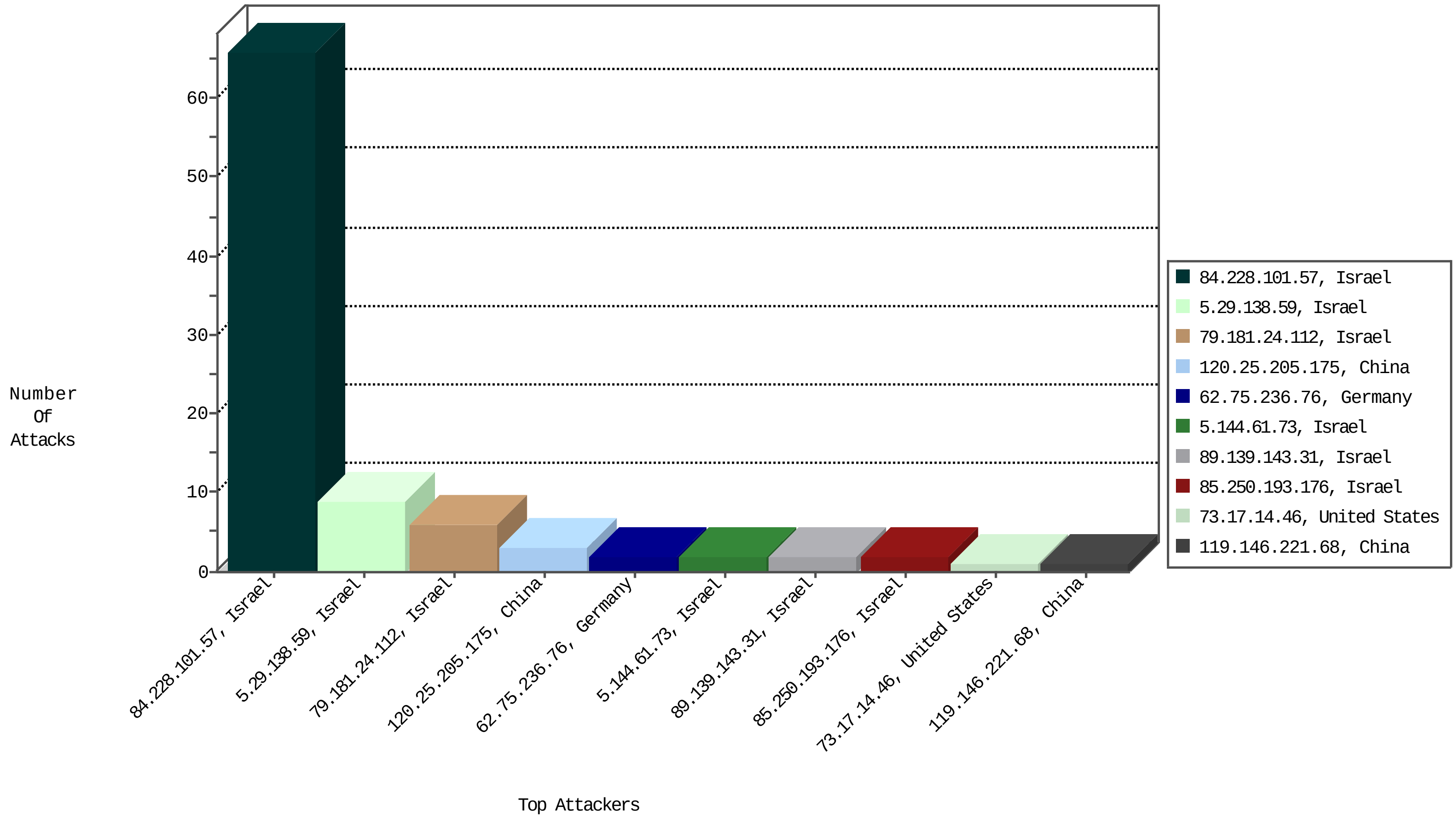
12-19-2015 to 12-20-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-19-2015 to 12-20-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
120.25.205.175	China	147.237.0.121		Frk_Under_Attack_Con_Http	drop	BBL-Frankfurt	2
120.25.205.175	China	147.237.0.121		Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	1

12-19-2015 to 12-20-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-19-2015 to 12-20-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
62.75.236.76	Germany	147.237.0.121		ET SCAN NMAP -sS window 1024	2
94.102.48.195	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
119.146.221.68	China	147.237.0.121		ET SCAN Potential SSH Scan	1
202.131.114.196	India	147.237.0.121		ET SCAN Potential SSH Scan	1
58.52.143.0	China	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
73.17.14.46	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
104.200.78.34	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
146.185.250.2	Russian Federation	147.237.0.121		ET SCAN Potential SSH Scan	1
218.108.132.58	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1

12-19-2015 to 12-20-2015

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	1352
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1215
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1090
149.88.145.181	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	684
84.228.101.57	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	347
109.160.165.59	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	252
2.54.8.29	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
149.78.244.19	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	183
149.78.41.170	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	180
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	179
149.88.150.186	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	161
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	154
109.65.75.215	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
79.25.232.148	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	140
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	124
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	123
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	121
40.77.167.7	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	115
149.78.145.135	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	103
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	72
149.78.31.17	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	69
108.171.129.189	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
149.88.7.255	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	47
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
149.88.90.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
149.88.166.167	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
66.249.73.156	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
5.102.254.191	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	23
5.102.254.191	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	23
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	22
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
149.88.226.27	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
125.25.32.122	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.93.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.73.174	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
192.114.23.18	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.102.9.22	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
31.168.19.88	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	12
66.249.73.156	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
157.55.39.194	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
157.55.39.214	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
66.249.69.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.228.101.57	Israel	147.237.0.121		Multiple Unknown HTTP Request Method from 84.228.101.57	Block	7
84.228.101.57	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Method from 84.228.101.57	Block	7
84.228.101.57	Israel	147.237.0.121		Multiple Malformed URL from 84.228.101.57	Block	7
84.228.101.57	Israel	147.237.0.121		Multiple Malformed HTTP Header Line from 84.228.101.57	Block	6
84.228.101.57	Israel	147.237.0.121		Multiple Abnormally Long Request from 84.228.101.57	Block	6
84.228.101.57	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Name from 84.228.101.57	Block	6
84.228.101.57	Israel	147.237.0.121		Multiple Abnormally Long Header Line from 84.228.101.57	Block	5
84.228.101.57	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Value from 84.228.101.57	Block	4
5.29.138.59	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	4
79.181.24.112	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.181.24.112 (sigalgs DoS Attack)	None	4
84.228.101.57	Israel	147.237.0.121		Multiple NULL Character in Header Name from 84.228.101.57	Block	4
5.29.138.59	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddDocs&FileToActivate in www.miluim-ishi.aka.idf.il/login	Block	3
85.250.193.176	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
5.29.138.59	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddDocs&FilesToCheck in www.miluim-ishi.aka.idf.il/login	Block	2
84.228.101.57	Israel	147.237.0.121		Multiple NULL Character in Method from 84.228.101.57	Block	2
5.144.61.73	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
84.228.101.57	Israel	147.237.0.121		Multiple Illegal Byte Code Character in URL from 84.228.101.57	Block	2
79.181.24.112	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
84.228.101.57	Israel	147.237.0.121		Multiple Illegal HTTP Version from 84.228.101.57	Block	2
84.228.101.57	Israel	147.237.0.121		Illegal HTTP Version	Block	1
46.19.85.90	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.95.50.188	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected C20390F4CBE9A7C4BC94460BD940C5FFADA1E83405D9A1496CA08F90304F9B70F0627288BE696BAB27163FF542D8DFF2F0CB58622C0BA3F6A5457717CFFFA97C4FEB0DAF4412D332773F78C79BCD73A59D6994AE2A424638154DD22B11254C13D7397D7A20124385EEA49443DC017DD4A881F96F9C020CFCA68AE5246E3732DA, Observed 520971AD2CD88367104E3CB1682E7D614DCF98ADCE243706F3738F95BC5953D4F527E1CE626B9431B317776422141EFC64FBEC46A891157189819CF9BCA8692D7784809538ACA6C7FD69B2AEF387F66BCF8FB9FAE6F34ABC82B9651A80C29AAFD8DCC8	None	1
199.203.122.61	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
84.228.101.57	Israel	147.237.0.121		NULL Character in Method Q07UxÂ‘6ÃºF;Ã•Ã¬FkÂ€ZXXvlÃºÃ¡Ã?ÃœÃ-Â”Â›[[#25]]aÃ,Â£ÃŸÃ¼J~[[#22]]7[O[[#16]]vÂžÂ¼Âž,bxKU*UÂ«Ãµ[[#19]]Ã›:Â’\Â±%Ã¦Â†ÃžÃ¥[[#26]]TÂ¢ikÂ‹@oÂŸMFÂŽ\KÃ?JÂ§[[#0]]UÂ¶Ãˆ[[#30]]Ã£Â†J[[#24]]q!Ã¸Ã£Ã·[[#30]]Â·Â…Â´Ã–Ã?eÃµ[[#11]]1[[#17]]'[[#26]]Ã¯EÃ¶Ã•Ã“Â˜Â„Â?Ã¶Âƒ&?Â?Ã Di)InÂ´[[#6]][[#6]]ÂŠÃ‘[[#8]]6Â•[[#17]]jÃ›Ã·f4Â¹ÃªÃ‡Ãˆ[[#25]]#`GWÂ˜v[[#18]])Ã–Ãµ[[#11]]Ã„Ã‘Ã?Â¹Âµ{ÃœÃŸVÃ eÂ„v[[#19]][[#15]]Â„Ã›Â‘Ã®ÂŽÃœ`Ã§[[#28]]Ã²Ã¸Ã,rÂ‡_Â¸Ã…Ã…Â??OÂ´Ã?Â‰Â‡Â¢%w4ÃºÃ¡f@[[#14]]Ã¹wÂŸ*v?MÃ’`[[#7]]d/ÃµÂ¼fÃˆÂ–`Ã?Â¨;nÃŽÃ¹Ã€}Ã	Block	1
79.177.116.75	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
5.29.151.169	Israel	147.237.0.121		Suspicious Response Code	Block	1
89.139.143.31	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 89.139.143.31 (sigalgs DoS Attack)	None	1
84.228.101.57	Israel	147.237.0.121		Illegal Byte Code Character in Header Value	Block	1
37.26.149.170	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
84.228.101.57	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.102.221.80	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
89.139.143.31	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.228.101.57 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
84.228.101.57	Israel	147.237.0.121		Illegal Byte Code Character in URL Â¿+j×–Â²'fË†+!0>â€¢'Ã»[[#28]][[#16]]ÃŸso	Block	1
46.19.85.0	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		Too Many Headers per Request - 30 Headers	Block	1
5.102.247.189	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
192.115.190.190	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
84.228.101.57	Israel	147.237.0.121		NULL Character in Header Name at	Block	1