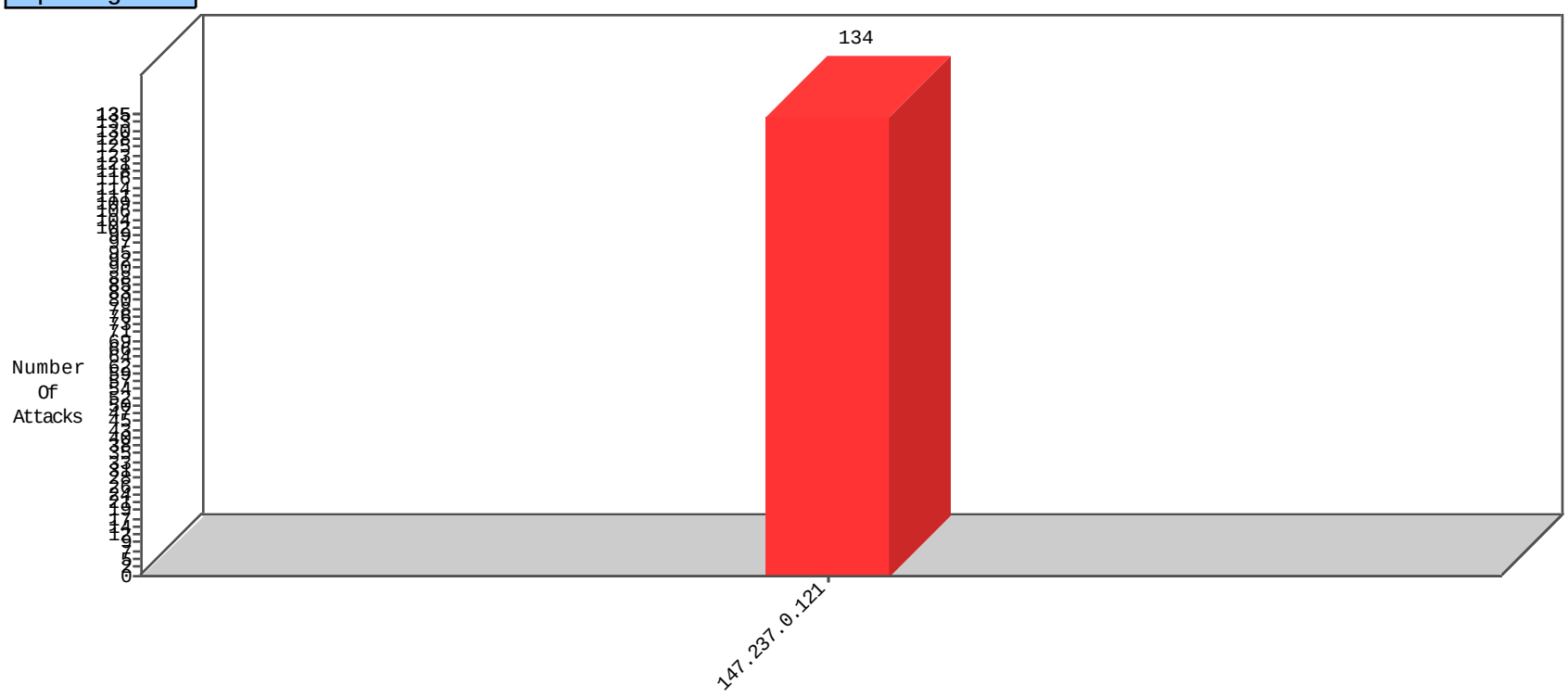
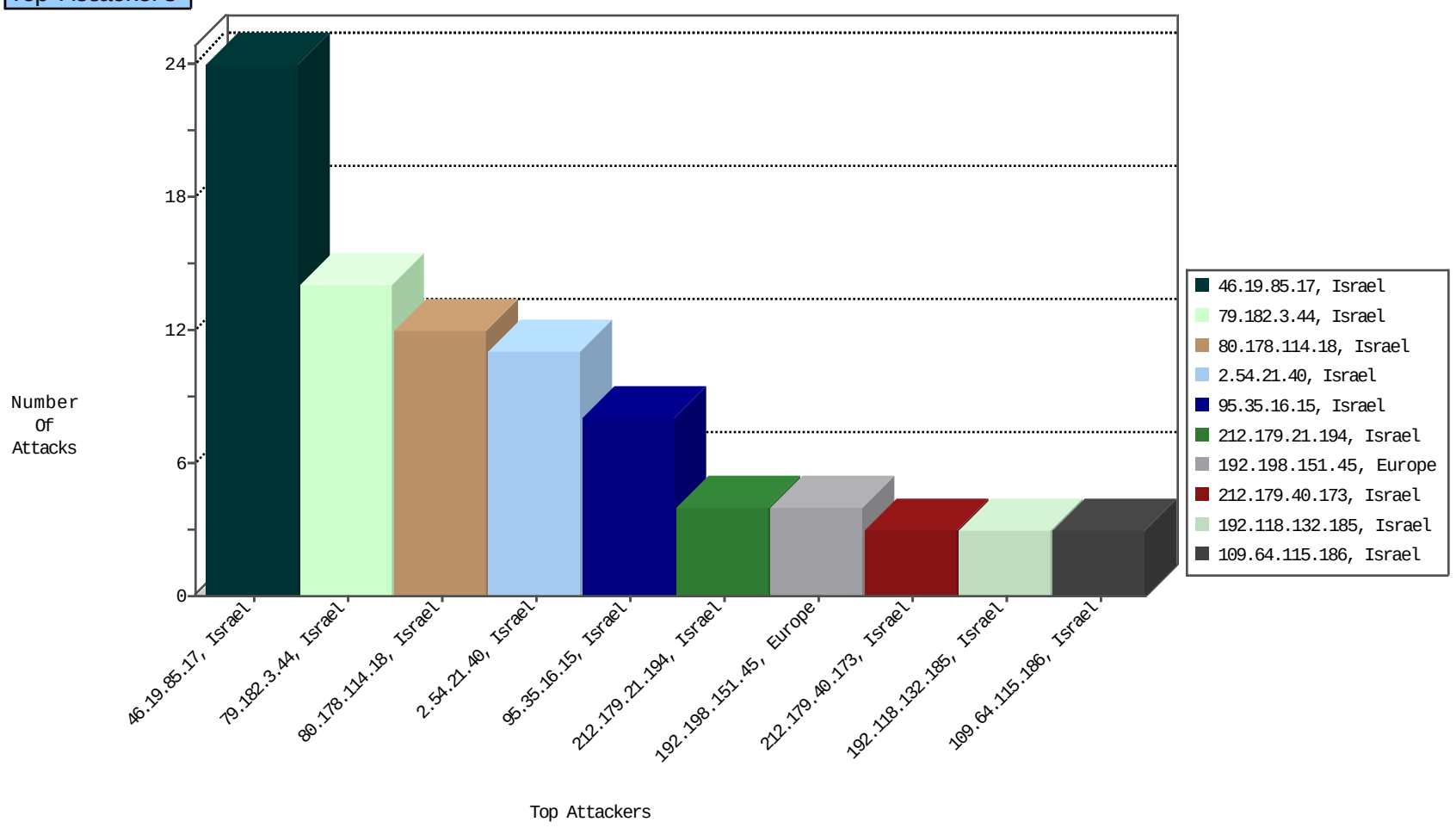
11-30-2015 to 12-01-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-30-2015 to 12-01-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
46.19.85.17	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	24
2.54.21.40	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	11
31.168.133.226	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
192.118.132.185	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
115.239.228.8	China	147.237.0.121		Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	1

11-30-2015 to 12-01-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-30-2015 to 12-01-2015

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)	4
115.194.42.134	China	147.237.0.121		ET SCAN Potential SSH Scan	1
62.245.45.132	Russian Federation	147.237.0.121		ET SCAN Potential SSH Scan	1
185.106.94.16		147.237.0.121		ET SCAN Potential SSH Scan	1

11-30-2015 to 12-01-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3604
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3321
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2976
140.101.20.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1806
155.94.185.161	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	980
208.87.233.201	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	705
149.78.27.128	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	468
149.88.224.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	432
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	340
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	317
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	309
149.78.30.195	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	296
94.16.11.27	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	280
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	277
149.88.20.28	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	253
109.66.54.3	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	224
2.54.41.103	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
2.54.131.3	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	146
79.178.121.8	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
80.246.139.237	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
16.16.16.3	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	125
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	119
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
149.78.41.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
193.186.163.3	Greece	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	97
149.88.89.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	93
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
2.54.21.4	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	81
208.54.70.224	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
66.249.82.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
2.54.9.3	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
149.78.221.136	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
2.54.131.3	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	49
2.54.131.3	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	49
207.232.36.181	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
2.54.131.3	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	49
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.88.29.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
82.166.53.161	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	38
149.78.27.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
2.54.182.223	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
84.110.108.37	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.54.177.255	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
66.249.81.129	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
80.178.114.18	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/$$$&?&?$$$	Block	12
95.35.16.15	Israel	147.237.0.121		Unauthorized HTTP Method	Block	8
79.182.3.44	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddBoardExamsPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	5
79.182.3.44	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	5
212.179.21.194	Israel	147.237.0.121		Suspicious Response Code	Block	4
176.13.0.219	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
212.179.40.173	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	3
87.69.174.78	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
79.182.3.44	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	3
109.64.115.186	Israel	147.237.0.121		Suspicious Response Code	Block	3
212.25.123.18	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.118.10.10	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.172.178.0	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 21EE229826C05728571A497FB63163C6F9D7E991C785941D48DD184E29839977F7F658DF682A049C09D70837D8CA869F2879F31E77780A50DF0F7E528A2754035239507428F60C3BDE97A78099019322102A347E86BA6B304B35557CB03462BCFB4941C451CDDD97A95E8CA49533F225CB1A333A2A8DB385F24978CC89C15268, Observed 8F1D2ACB485360187CCBDA052B8F855E60E564650456BBD6D5BA7D1EBC5049C43CF690E371B763DE316E23FD36C7F81FFA39B16FB6C53534220C564F959592B99E9E7C4A3CF94520242BCC1C47CDE7C94A79B572B7B2E6B5F053B0B554972A36447C01	None	2
194.90.128.185	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
79.180.186.211	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.180.186.211 (Unknown SSL Session)	None	1
93.173.132.10	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.108.209.80	Israel	147.237.0.121		Multiple Unauthorized URL Access from 84.108.209.80	Block	1
46.116.234.65	Israel	147.237.0.121		Unknown Parameter zi in www.miluim-ishi.aka.idf.il/login	Block	1
192.114.105.254	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.64.169.164	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
87.69.34.98	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
80.246.136.10	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/newpassword/	Block	1
194.90.128.185	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
79.180.186.211	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
176.13.8.181	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.71.113	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 85.250.71.113 (Unknown SSL Session)	None	1
213.8.111.131	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
79.179.17.144	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
192.115.190.190	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.65.56.199	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
81.218.140.248	Israel	147.237.0.121		Unknown Parameter ma in www.miluim-ishi.aka.idf.il/login	Block	1
79.180.186.211	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
5.102.217.252	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.106.226.31	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
109.64.113.216	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected EBBD32F45D9CF492D06F3826745BD733C5B77F7292D28CD43EEA714E05B3BE8AC672B2D2DBCD5A06EEF1111CEB3DC553E17ABCD7F10A0C73696EC046AF1753EEED36FB22B9BC57096682526C7718F97668226DF30614D84C344A3216107150D0ACD055405FFAB84AEB1B53A75D38F60F647B468BA3829991C4721D56632C68EA, Observed 98A054587B4B0BA478A82E30DBD4D383937EC43829B3CC67BE28D902AE818A98B95A0D6F31E250EB4A7A57E87267551CE0D61BE1A4905B03A29E6681B3E37404B3FAC808EECB8F9C71C2C6D7FC13795502D49C34665168E73CEFFE6D1DDE344A90C68B	None	1
85.250.71.113	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
79.182.3.44	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
79.180.168.12	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00$txtNewPass1 in www.miluim-ishi.aka.idf.il/personalsettings	Block	1
109.186.20.183	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 79BFD6606FEEFC015249DE091FCE19D71BA1EFF01DB01C610771D0E6E19765BFF3FD29EC2F9B133793FD5448D95E95E348EA599FA8900CBE5825B3E2DFC0887770BA1789216562A436A31BC21AD131055E8BCD28F14DC7615E50F59970F112DC50839BD99D45C3D02EB54E54D8D4CE47A2D2B50B38A2D40BF850AA18692986CA, Observed 143D5424898F2A442E3A49199D5D746BD2FFA23B22A31436A5F8ACD350E15D7CB8D5E82FC7E456E7266F90677C15D95F09D074BB591A23D51BE084B139D6DDD2B0537C6938896CAD616CCB772C13C6F2FEB2334A1C788BF5EA7EA5B309EA90ACE3189A	None	1
81.218.144.209	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.149	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.114.87.9	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
85.250.71.113	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1