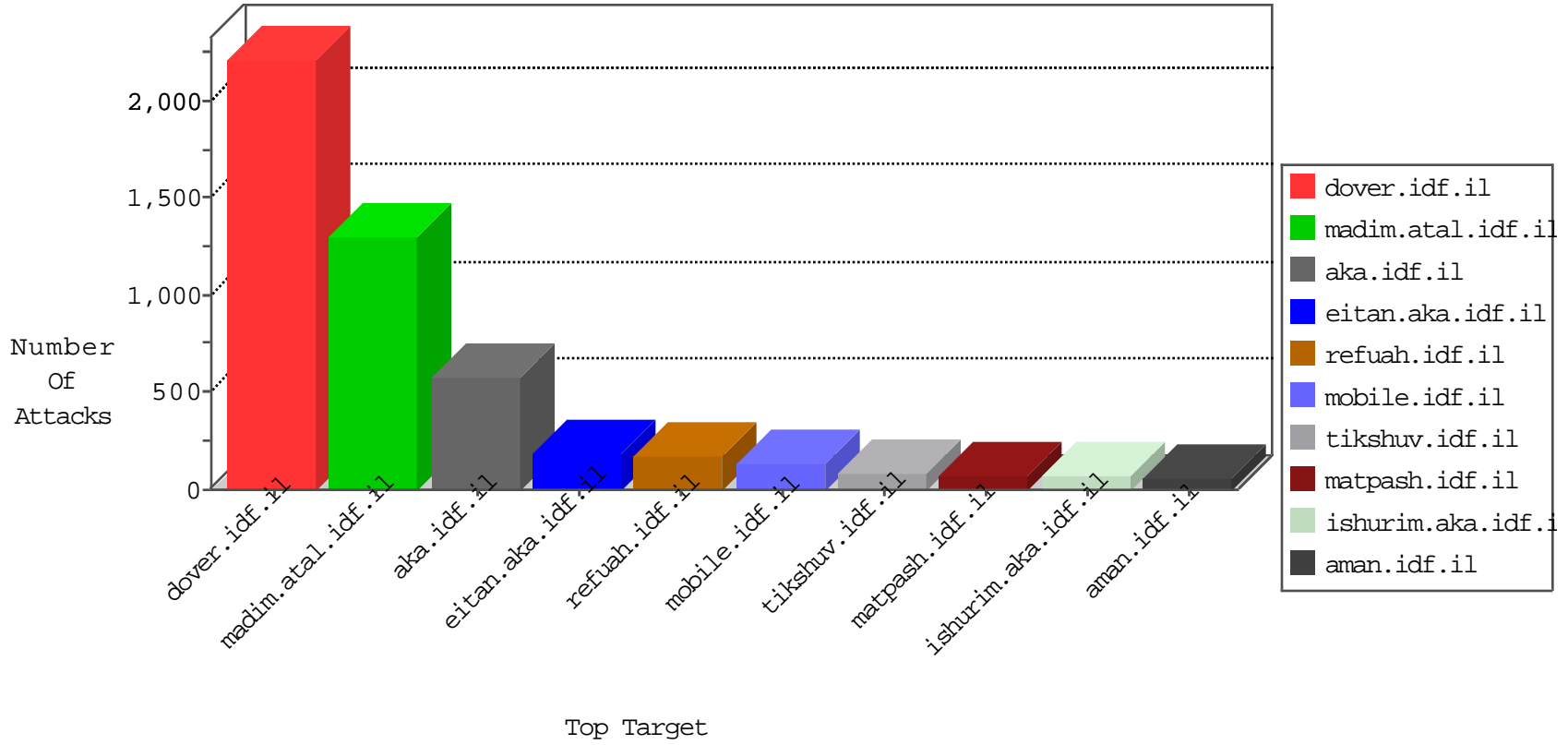


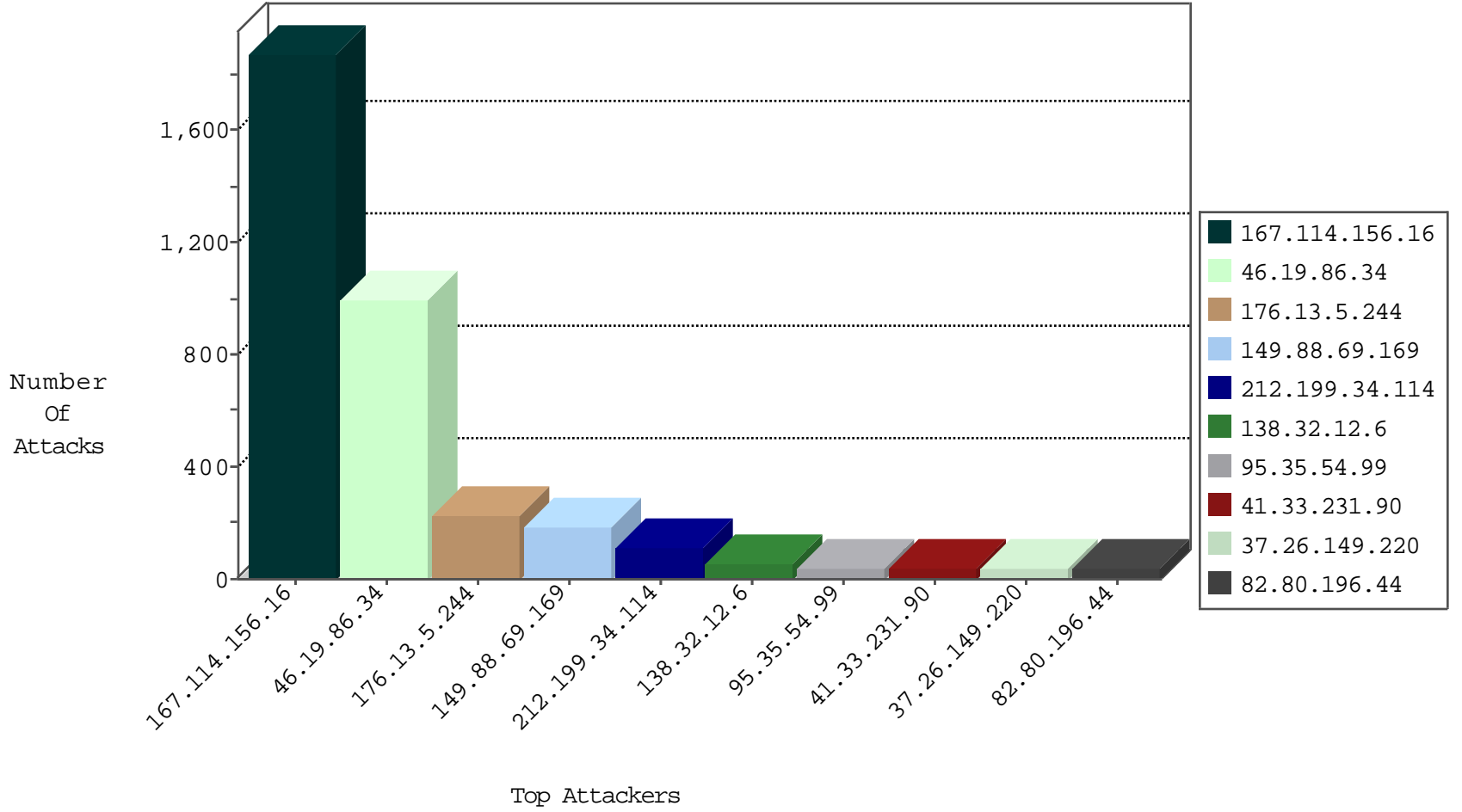
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3070
46.19.85.73	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	10
109.66.174.29	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
80.246.133.47	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
107.150.98.125	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
23.95.248.111	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.88.154.138	Poland	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
195.74.38.14	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
73.179.208.124	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.74.38.14	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
146.185.250.2	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.165.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.199.34.114	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	111
138.32.12.6	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.149.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.54.62.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
199.30.24.116	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
95.35.54.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
176.13.5.244	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
176.13.20.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
23.91.70.94	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
37.26.149.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
2.54.50.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.127	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
5.28.189.36	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.89.217.232		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
82.80.196.44	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.21.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.66.206.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.89.217.230		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
87.68.249.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
95.35.54.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
79.182.115.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
95.35.54.99	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
185.89.217.231		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.154.149.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
176.13.9.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.154.149.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.149.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
81.218.143.30	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
77.125.13.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
82.80.28.7	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
31.154.149.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
185.89.217.225		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.187	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.177.155.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.80.196.44	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
147.235.185.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.130	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.180.62.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
149.88.220.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.181.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.150.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
79.176.124.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.228.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	582
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	362
149.88.69.169	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
176.13.5.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	108
176.13.5.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.34	Block	49
46.19.86.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
176.13.16.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
2.54.154.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
37.26.149.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.62.77	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.20.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
124.146.201.2	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 124.146.201.2	Block	4
2.54.188.198	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	4
176.13.9.123	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.50.71	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.253.134.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.183	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
5.29.228.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.102.216.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	2
80.246.139.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.2.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.22.134.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	2
79.181.184.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	2
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
37.26.148.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.116.129.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.197.140	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
87.69.109.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code Custom_Temporary	Block	1
2.54.58.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
176.12.139.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.210.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
23.91.70.94	United States	147.237.72.166	aka.idf.il	Multiple signatures from 23.91.70.94	Block	1
109.65.97.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.90.76.185	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.32.179.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.139	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.175.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1