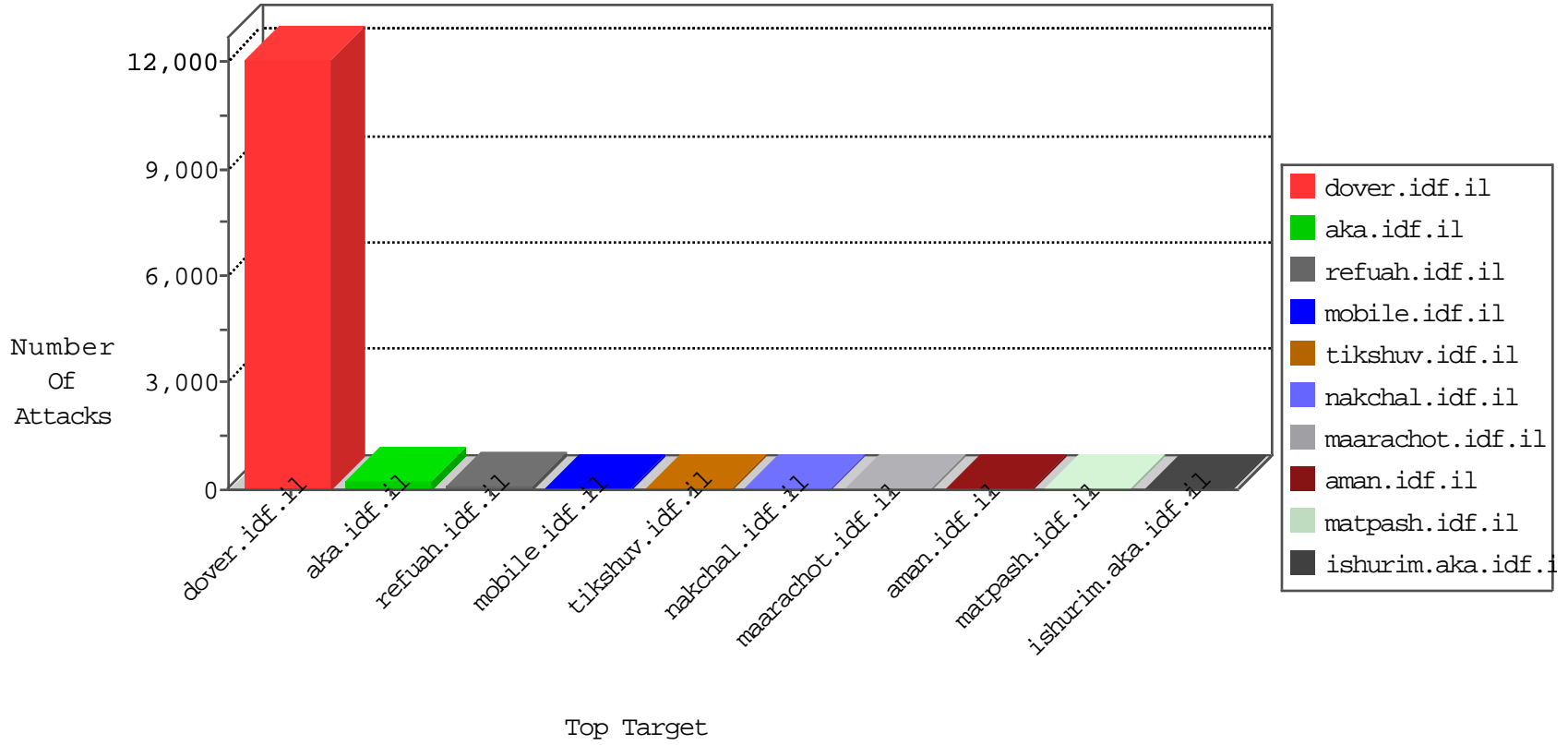
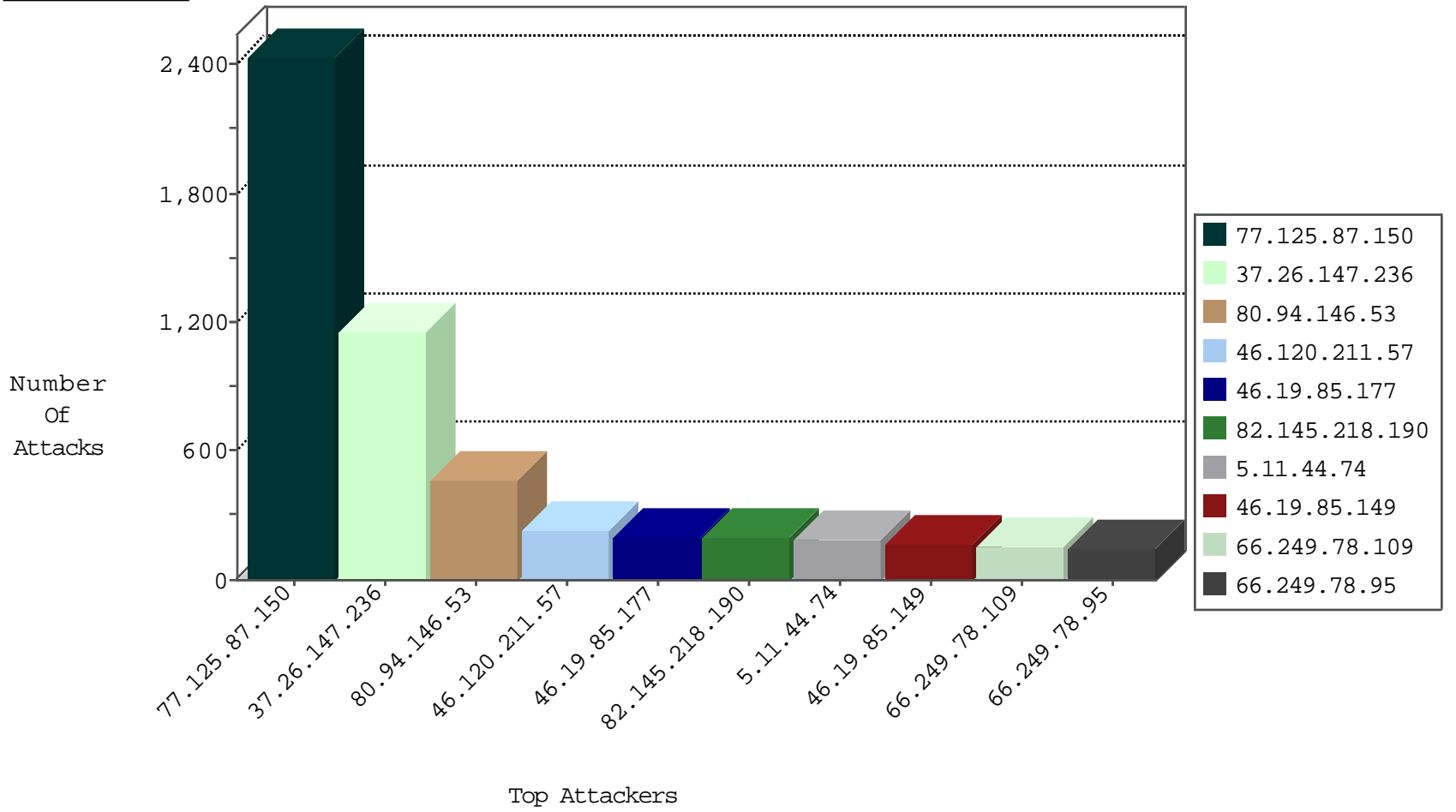




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.160	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	109
87.69.149.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	69
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
62.128.48.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
212.76.108.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
46.19.85.255	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
79.176.98.224	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
222.186.21.109	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
37.26.147.214	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
199.203.172.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.150.237	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
183.179.33.228	Hong Kong	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
217.33.142.242	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.180	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
210.165.101.233	Japan	147.237.76.176	test.noore.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
109.66.200.8	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.87.150	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2426
178.115.129.48	Austria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
84.109.101.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
2.54.13.46	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.215	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.37	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
37.26.146.249	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.151	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.156	anan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.120.148.179	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.108.80.149	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.68	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
86.71.159.85	France	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
176.12.148.255	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.12.175	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	Italy	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
109.67.189.254	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.93.181	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.128.193	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.151.94	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.15.40	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
203.194.234.109	Hong Kong	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
77.125.87.237	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	United States	147.237.76.177	ncore.idf.il	ET DROP Dshield Block Listed Source	1
37.26.148.160	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.176.56	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.167.139	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	Italy	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
2.54.142.109	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.96.133	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
95.173.171.236	Turkey	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.159.155.53	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.178.222	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.134.129	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.221.145	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
199.231.185.135	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
46.117.89.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
188.95.158.198	Ukraine	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 3072	1
5.255.85.233	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.26.147.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1152
80.94.146.53	Switzerland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	468
46.120.211.57	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	232
82.145.218.190	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	198
46.19.85.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	198
5.11.44.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	183
46.19.85.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	167
77.127.72.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	143
197.133.30.230	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	141
94.228.34.250	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	132
2.54.171.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	116
109.75.66.60	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	112
212.179.61.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	94
46.19.86.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	85
66.249.78.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	85
66.249.78.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	83
212.179.61.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
66.249.78.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	77
109.160.188.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
205.203.117.2	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
176.12.143.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
107.170.144.19	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
2.54.177.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
77.125.49.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
82.80.60.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
109.65.57.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
66.249.78.109	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
79.183.120.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
46.19.86.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
31.168.83.32	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
46.19.86.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
66.249.78.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
176.12.146.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
176.12.143.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
91.135.102.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
5.29.12.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
37.142.154.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
66.249.78.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
2.52.187.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
149.78.107.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
138.134.102.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
176.12.138.254	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
95.91.225.126	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
194.90.25.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.146.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
213.151.48.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
82.166.134.94	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 82.166.134.94	Block	7
149.78.69.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
80.246.135.51	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.135.51	Block	4
206.217.77.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
79.176.132.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.12.138.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.25.121.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.54.54.192	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
46.19.86.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
89.138.20.53	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
192.114.23.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	2
212.150.119.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
82.166.134.94	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/6_s3_	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Malformed URL from 202.112.50.77	Block	1
185.32.177.64	Israel	147.237.77.243	mobile.idf.il	Cookie Tampering on cookie __RequestVerificationToken_Lw__: Expected AoMYxWnk6GBJnQpJdmBsQ19kcgd+Q/Z3JhffY1UXcJ3kduBtWnUUyQFgSylEiIK58X2DtaHmwX9gKDP7aQbyNvVDFJaMxA7baJqJWgSElZthfu20bAldLQ60BZCO0lkKAoagJ2C11HqyB9wz7ASdaGQJN28jtZe2gwQgwHza4=, Observed YpOilUzZqCGil8oN57cvFLdLbKxyRITCbP2hY7G7Io5zDoTVJEMZuljWLFeswxxI749KnlSjkEtlLKublCFYKenGRLbkm5KQMIJFBTtiaCgptt04j1UE9snv8rqkBTBUQy3dk/V+WessMLo2h086hiUSla54+KmEdjBkcku7WJ4=	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	1
109.64.111.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$cpSachar\$ct155 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
45.33.69.56		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 194.114.146.227 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
68.180.228.251	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
180.76.4.97	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
66.249.64.71	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71521-he/maarachot.aspx	Block	1
213.151.43.223	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/...	Block	1
85.65.33.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.147.178	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 202.112.50.77	Block	1
79.180.234.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
188.138.17.205	France	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
176.12.139.71	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
212.117.143.250	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
109.64.146.182	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
5.29.191.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
198.20.69.74	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
80.246.135.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
180.76.5.147	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/901-7724-he/tikshuv.aspx	Block	1
66.249.64.74	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
157.55.39.9	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8601-he/navy.aspx	Block	1
87.69.125.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//www.tikshuv.idf.il	Block	1
37.142.92.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1
188.165.15.94	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
80.178.158.133	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.140.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1