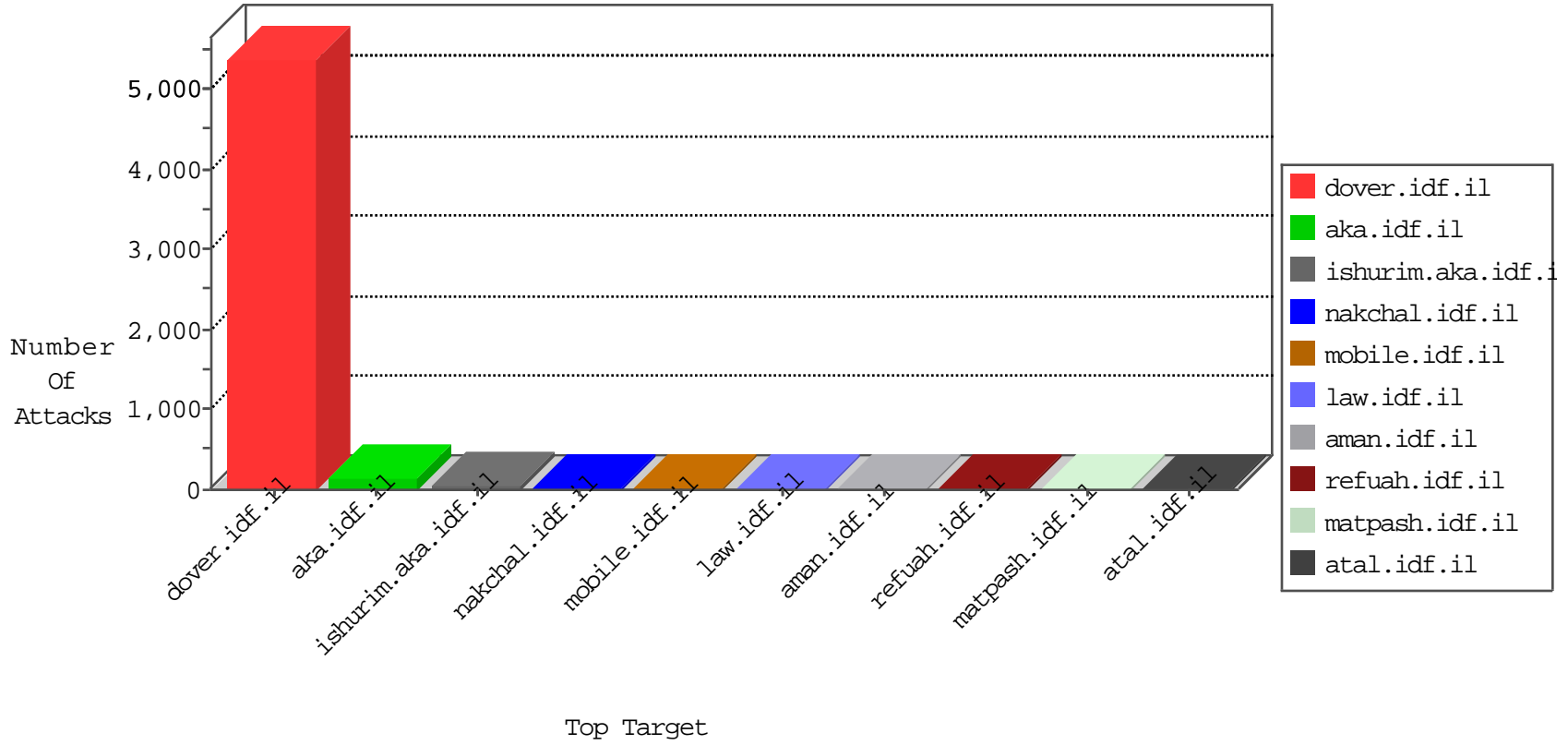
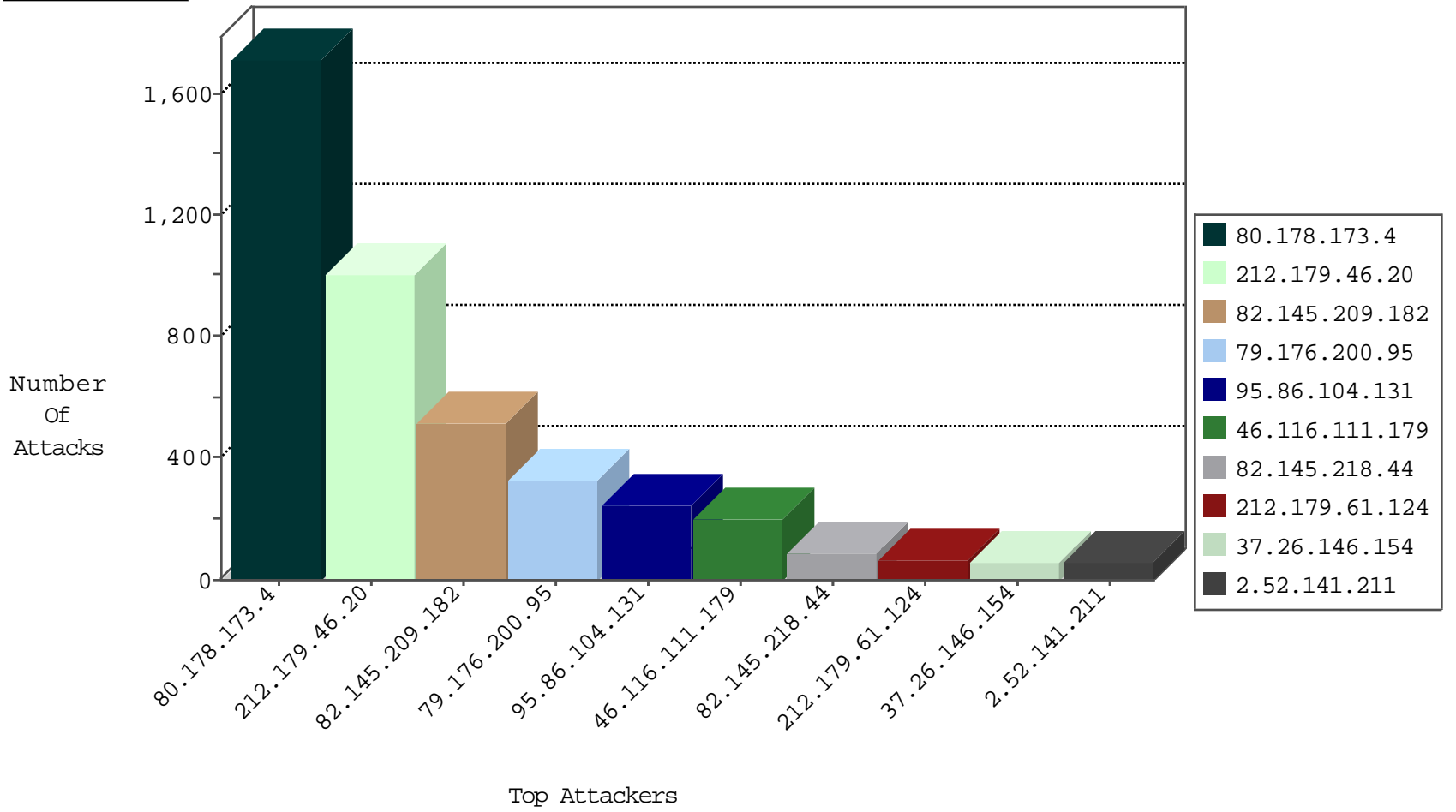


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
188.161.79.41	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2917
46.120.80.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
46.19.85.188	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
81.218.97.114	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
138.134.102.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.80.219.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.179.33.145	Israel	147.237.72.167	ishurim.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
124.232.142.220	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
2.52.43.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.29.232.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
58.153.126.206	Hong Kong	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
85.64.230.176	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
91.227.165.5	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
31.168.133.168	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
5.29.198.16	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
109.67.190.187	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
109.226.20.135	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
198.20.70.114	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.93	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
132.66.231.248	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
185.22.224.96	United Kingdom	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
81.218.177.180	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
132.76.50.6	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
62.219.121.213	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.70.114	United States	147.237.77.178	e.matpash.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
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
134.93.84.135	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
91.227.164.5	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.noore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
93.115.85.34	Anonymous Proxy	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
77.125.129.83	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
37.26.146.180	Israel	147.237.76.42	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
85.65.100.101	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.149.114	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.130	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.13.186	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.174.147	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
122.252.230.36	India	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 3072	1
85.250.221.9	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.255.67	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
212.150.133.226	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.69.227	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.17.187	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
115.68.23.201	Korea, Republic of	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
80.178.173.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1711
212.179.46.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	987
82.145.209.182	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	514
79.176.200.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	327
95.86.104.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	246
46.116.111.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	200
82.145.218.44	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	85
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
2.52.141.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
82.25.173.183	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
79.179.149.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
46.19.86.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
77.246.195.65	Finland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
46.117.75.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
107.145.100.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
37.142.156.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
185.26.182.38	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
101.171.170.168	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
37.26.146.154	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	alert	19
37.26.146.154	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	19
37.26.146.154	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid sequence number	Bad TCP sequence	monitor	19
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
2.52.42.174	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
109.253.157.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
213.244.81.60	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	13
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
82.109.66.147	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.19.86.250	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	12
46.19.85.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
185.26.180.138	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
212.179.46.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.81.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
85.64.230.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
82.109.66.150	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
82.80.216.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
207.232.37.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
132.76.50.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.168.207.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
212.150.79.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.177.171.70	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
82.109.66.151	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
87.79.200.107	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
212.235.58.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
85.25.136.37	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.25.136.37	Block	5
79.182.131.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.176.14.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
194.90.88.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	3
85.65.22.224	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.72.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
84.94.54.87	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.121.247.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
95.86.64.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/6_s3_	Block	1
80.179.225.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//www.tikshuv.idf.il	Block	1
5.28.184.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.116.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
109.65.99.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/common/includes/bignewsrnd.asp	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.116.72.214	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/6_s3_	Block	1
207.46.13.118	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/contactform/contactform.aspx	Block	1
79.177.171.70	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6366-he/patzar.aspx	Block	1
52.5.88.49	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
80.246.130.91	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
5.29.198.16	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.237.138.51	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
178.49.154.17	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
109.66.157.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18489-he/dover.aspx	Block	1
85.250.79.138	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
46.116.163.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.42.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.42.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.52.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.93.142	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/scriptresource.axd	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.6.3.110	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
95.86.104.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.68.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx	None	1
79.176.14.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.14.139	Block	1
180.76.4.108	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
109.253.158.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-13725-en/dover.aspx	Block	1
46.117.239.72	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.174.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.93.146	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/webresource.axd	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/general.aspx	Block	1
62.219.47.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	1
109.64.108.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
31.168.84.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1