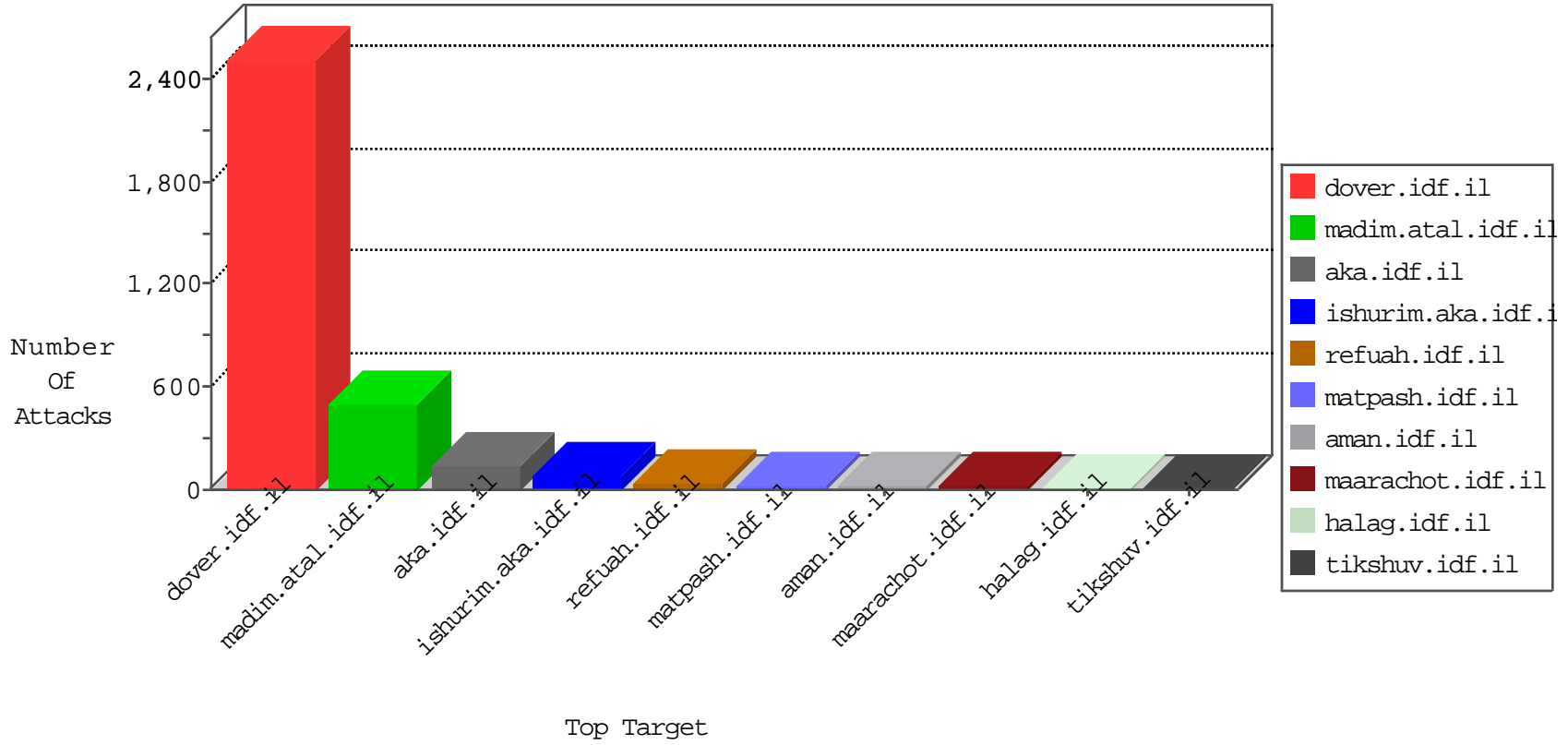
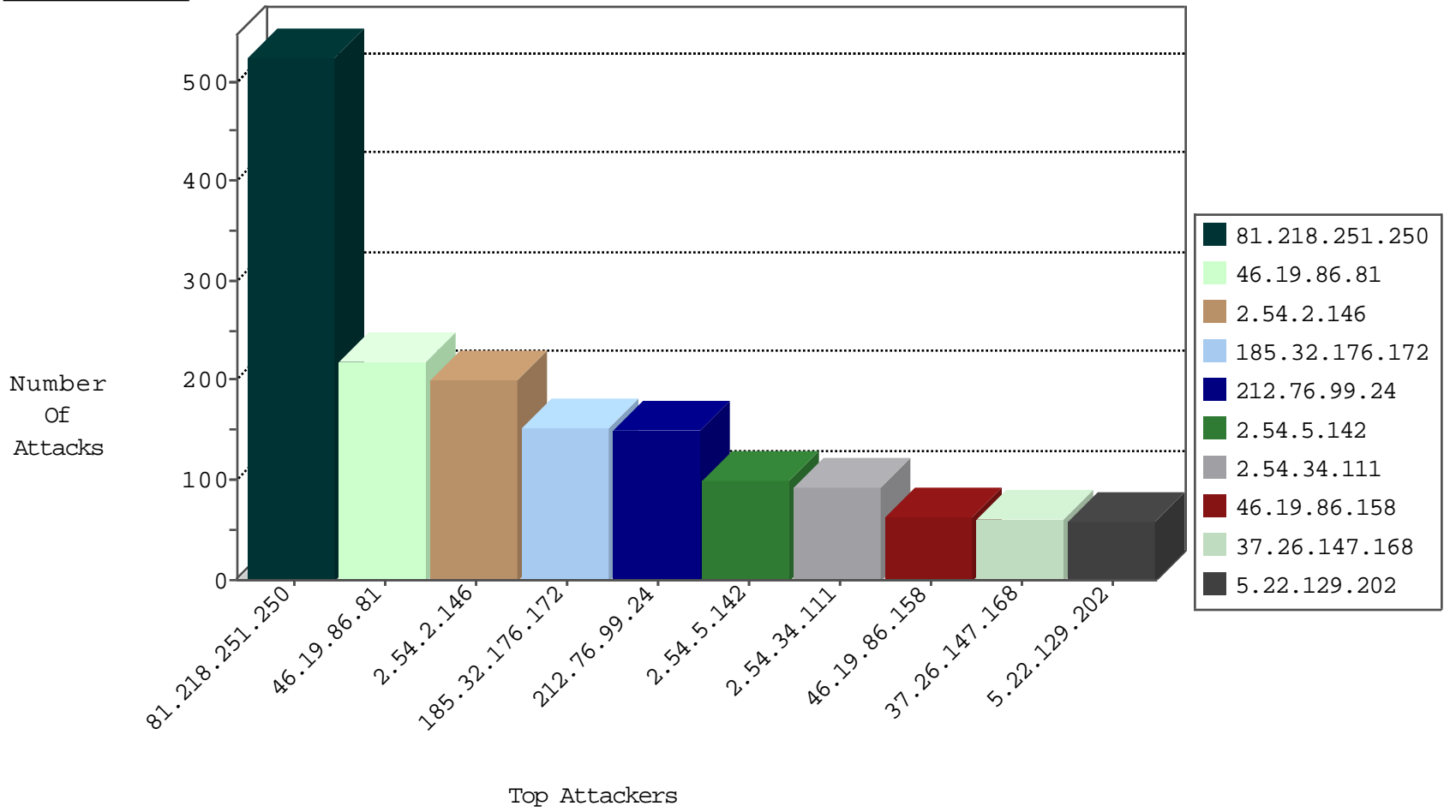


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3179
85.64.135.231	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
195.244.23.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
2.54.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
84.95.211.150	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
81.218.56.230	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
87.68.87.74	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
81.218.97.45	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
85.64.20.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
138.134.102.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
87.68.84.73	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.53	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.179.2.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
50.156.164.35	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.146.164	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
121.9.244.240	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	1
54.72.73.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
67.190.226.109	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
213.128.75.76	Turkey	147.237.0.200	m4u.idf.il	I4 Source or Dest Port Zero	drop	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
2.54.9.150	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
79.182.162.87	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
50.7.159.11	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
79.197.184.111	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
62.219.150.167	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.156	aran.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.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
37.205.9.131	Slovakia	147.237.72.156	aran.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.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
71.6.167.142	United States	147.237.77.235	sviva.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
212.199.169.17	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
109.253.140.251	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.28.59.150	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.172.128.157	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
2.54.9.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.182.91	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
81.199.120.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.69.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
80.255.10.229	Germany	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.179.227.21	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.40.173	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.77.4	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
58.20.54.249	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.136.254	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
222.229.31.116	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.133	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.28.59.150	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
37.142.191.223	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.164.85	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
31.7.57.198	Switzerland	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.188.188	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
91.231.192.149	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
2.52.6.64	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.44.137	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
80.255.10.229	Germany	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.246.206	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.125	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.61.122	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
207.232.35.188	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.12.137.173	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.101	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.18.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
222.229.31.116	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.70	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	525
2.54.2.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	200
212.76.99.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	151
2.54.34.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	92
46.19.86.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	62
37.26.147.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
95.86.78.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
2.54.170.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
79.182.27.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
37.26.146.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
46.19.86.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
5.22.129.202	Israel	147.237.72.167	ishurim.aka.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	29
185.71.140.48		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
46.19.85.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.253.87.226	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
212.179.61.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
5.22.129.202	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	25
176.12.143.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
79.181.131.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
81.218.159.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
109.253.142.176	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
94.159.157.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
79.178.184.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
212.179.42.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
212.199.135.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.121.69.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
95.86.113.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.121.138.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
79.183.5.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.199.57.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
46.116.189.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.159.174	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
46.19.86.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
5.102.224.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
109.65.21.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
62.0.101.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.168.92.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.116.112.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.168.101.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
192.115.248.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
109.253.143.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
89.139.9.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.94.181.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	218
185.32.176.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
2.54.5.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
80.246.137.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	11
194.90.66.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	9
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	7
213.151.44.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/undefined	Block	5
216.246.23.156	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
2.54.32.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	4
5.29.154.87	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 5.29.154.87	Block	4
46.253.87.226	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
198.98.181.100	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
46.19.85.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
176.12.142.173	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.12.142.173	Block	2
81.21.67.58	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
176.12.142.173	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
193.169.188.90	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
198.98.181.100	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
91.234.34.253	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
216.246.23.156	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
79.176.100.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
192.169.59.190	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
67.222.147.73	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
213.57.212.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
189.113.2.194	Brazil	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
216.246.23.156	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	2
2.52.152.62	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
91.234.34.253	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	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
213.151.35.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
91.228.248.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
66.249.64.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
192.114.23.211	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-welcome.stm	Block	1
79.179.164.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	1
212.179.23.29	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.99.145	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
193.169.188.90	Ukraine	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
77.125.167.121	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
37.26.147.203	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
188.143.232.13	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
132.68.80.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
213.151.44.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.64.70	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
198.98.181.100	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
91.234.34.253	Ukraine	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1