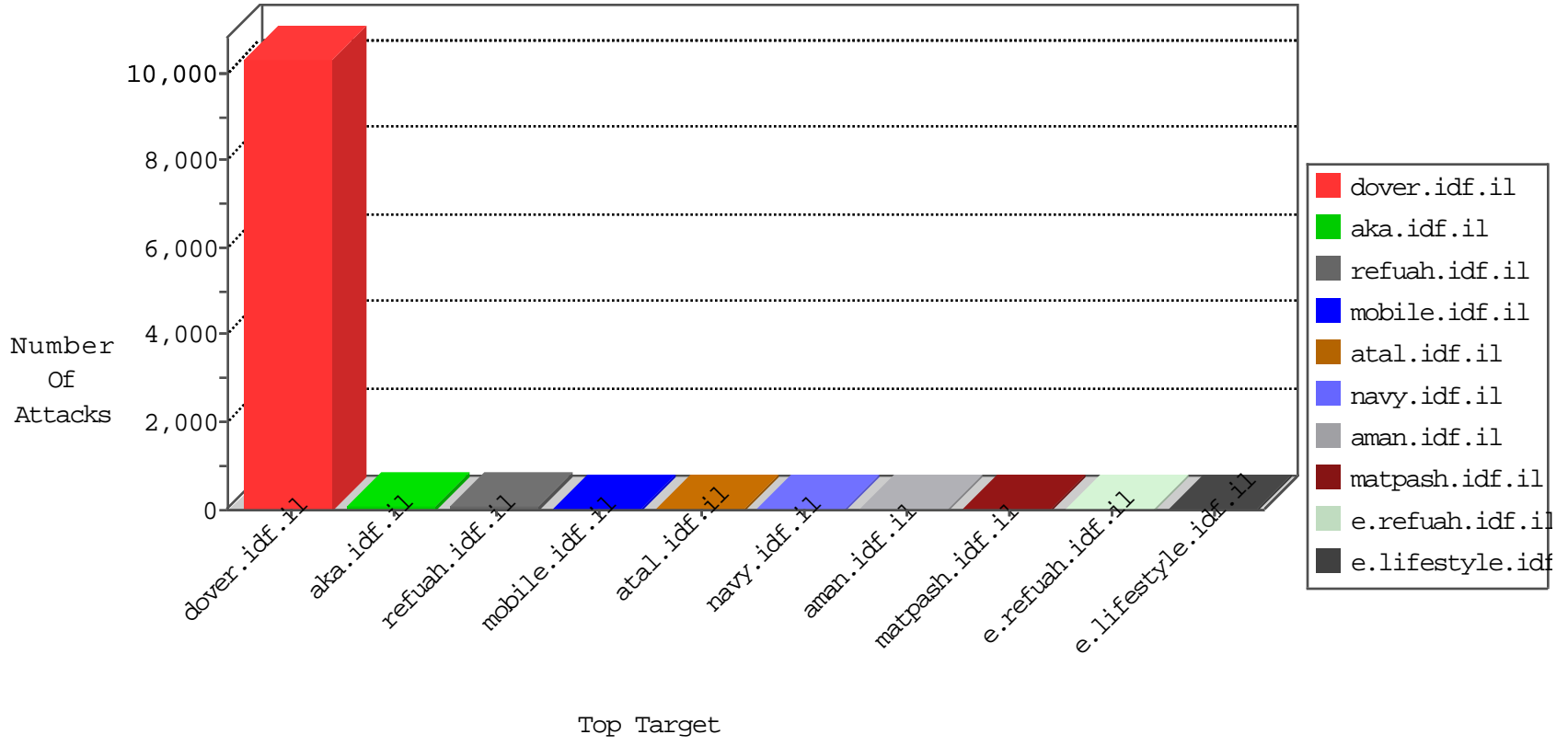
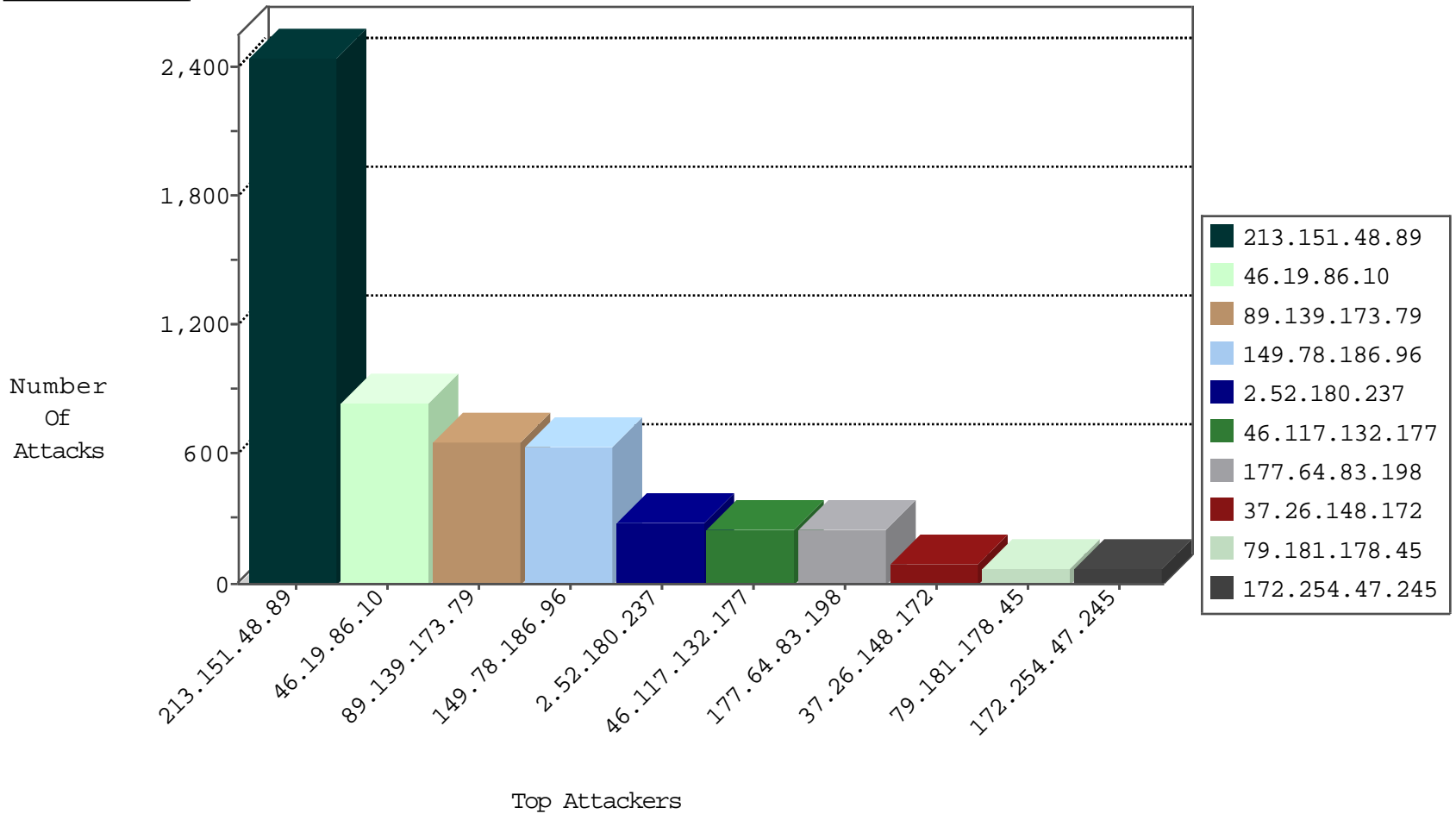




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3170
220.181.108.153	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	402
220.181.108.163	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	156
220.181.108.90	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	68
220.181.108.81	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	45
24.152.150.87	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
192.168.1.103		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
84.111.182.95	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
149.78.172.18	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
89.139.180.181	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.181.102.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
2.54.169.222	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.54.169.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.228.51.188	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
79.183.150.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
5.29.110.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
87.69.148.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
84.94.179.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.142.152.247	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
23.229.51.42	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
176.228.159.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.253.135.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
23.229.51.42	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
109.253.147.188	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.94.179.12	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
213.151.60.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.180.137.183	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.102.254.16	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
87.68.152.88	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	2
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.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
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chimuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
108.27.90.82	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
5.28.164.17	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
85.65.140.254	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
79.177.198.14	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
199.101.186.200	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
195.245.175.243	Portugal	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.175.243	Portugal	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.70.230	Netherlands	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.175.243	Portugal	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
79.176.26.134	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.175.243	Portugal	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
213.151.48.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2445
46.19.86.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	837
89.139.173.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	658
149.78.186.96	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	634
2.52.180.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	282
46.117.132.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	253
177.64.83.198	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	251
37.26.148.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	91
79.181.178.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
172.254.47.245	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
107.205.236.28	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	62
2.54.32.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
81.218.187.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
84.228.42.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
74.128.86.36	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
188.227.166.187	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
79.180.188.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
79.181.102.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
109.253.146.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.134.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.157.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
46.20.210.72	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
84.228.51.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
109.253.134.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
84.228.137.11	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	32
5.28.158.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
109.65.68.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
5.29.231.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
84.228.139.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
212.199.109.234	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	26
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
5.29.190.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
89.139.33.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
79.181.117.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
109.253.158.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
79.177.120.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
79.183.4.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
176.12.137.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
213.57.135.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
164.138.117.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
87.68.34.255	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
5.28.142.72	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
213.151.43.203	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
46.19.85.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigation.asp	Block	4
79.178.109.108	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
37.26.147.223	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
37.142.248.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
85.158.203.5	Netherlands	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
109.66.3.108	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
85.158.203.5	Netherlands	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
77.127.18.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17923	Block	1
95.86.127.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
84.111.25.238	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmilui/templates/inner.asp	Block	1
149.78.151.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.64.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/giyus/faq.aspx	None	1
77.127.144.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
212.199.109.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 46.117.164.60 (Unknown Server Certificate)	None	1
84.228.47.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/x@x\$*xax™x^ 3	Block	1
157.55.39.178	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
109.66.171.245	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
84.228.137.11	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
72.46.132.114	United States	147.237.76.86	navy.idf.il	Admin Blocking	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
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/homepage.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
93.172.172.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
79.181.163.234	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	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	1
109.67.103.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.73.15	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/main.asp	Block	1
31.168.201.87	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
85.64.163.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
72.46.132.114	United States	147.237.76.86	navy.idf.il	Multiple Admin Blocking from 72.46.132.114	Block	1
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
188.165.15.224	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
95.86.83.206	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.19.85.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
84.108.218.149	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/main.asp	Block	1
109.67.134.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigation.asp	Block	1