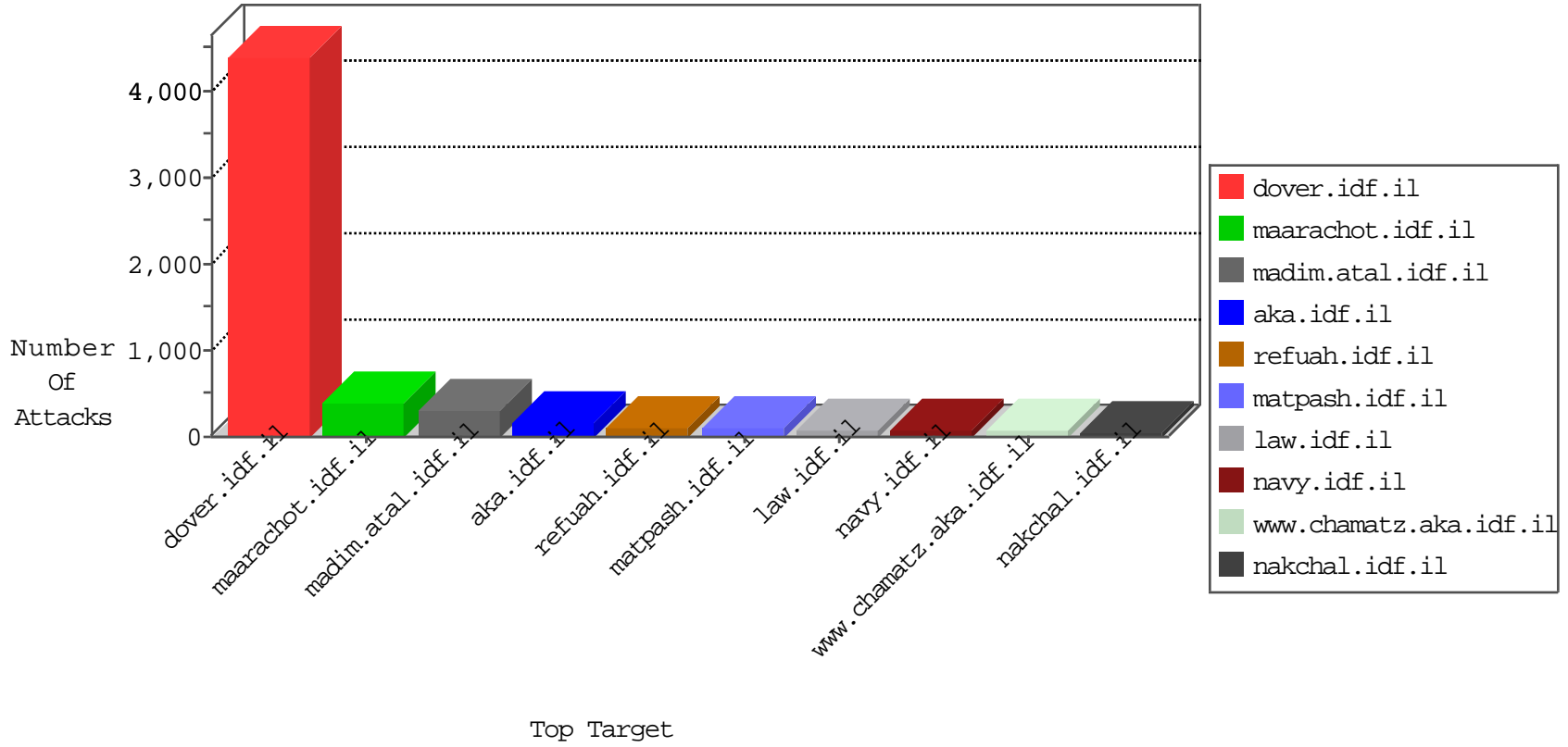
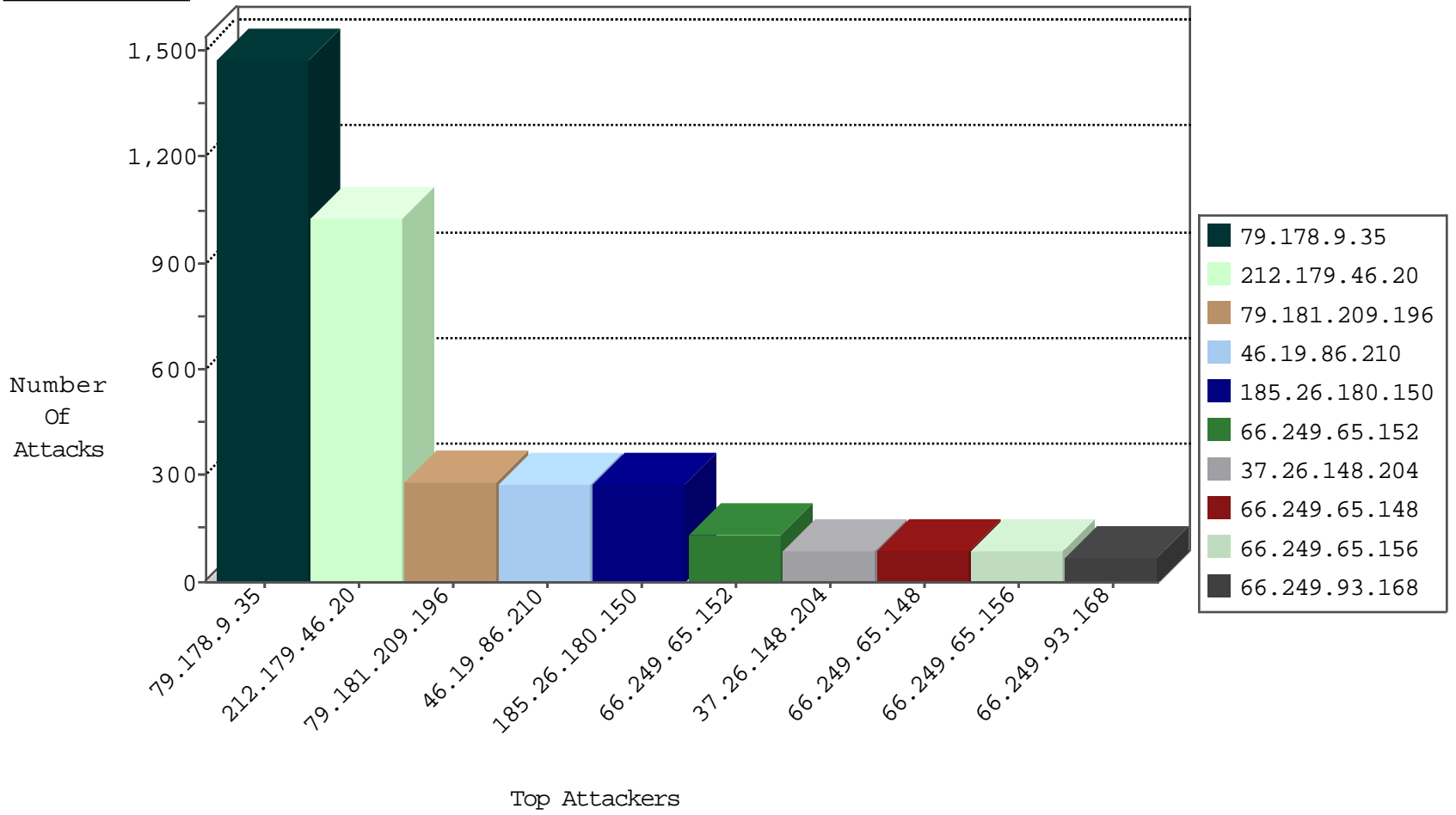


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.107	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	2958
84.228.247.242	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	487
84.110.60.143	Israel	147.237.72.156	aran.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	130
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	87
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	85
109.66.56.196	Israel	147.237.72.156	aran.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	69
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	67
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	45
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	38
66.249.65.195	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	36
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	35
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	33
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	32
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	29
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	27
66.249.65.187	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	25
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	24
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
66.249.65.191	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	23
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	21
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
66.249.73.217	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	21
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	20
66.249.73.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.64.55	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	17
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
66.249.64.63	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	14
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	13
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
66.249.64.87	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	11
37.26.147.146	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
66.249.73.201	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.73.132	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.73.244	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.80.75	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.64.79	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.73.140	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.135.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.38	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
207.225.131.141	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
77.125.146.3	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.76.200	eitan.aka.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.0.19	madim.atal.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.76.202	e.halag.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.0.35	akaws.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.77.19	law-forum.idf.il	DVRep_P-N_40-59	Permit	1
46.19.85.31	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.8.14	e.orchot.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.72.14	dover.idf.il(old)	DVRep_P-N_40-59	Permit	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	doover.idf.il	Tehila - Perl LWP with fake user agent	7
61.240.144.64	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.141	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
210.252.145.146	Japan	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.141	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
167.88.41.228		147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.141	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
167.88.41.228		147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.141	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
104.209.35.48		147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
84.108.94.128	Israel	147.237.0.15	kosher-kravi.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 Ddos attack	1
43.255.191.141	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
69.12.92.160	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
210.252.145.146	Japan	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.141	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
167.88.41.228		147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.141	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
125.5.16.195	Philippines	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.221	Netherlands	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
81.248.22.178	Guadeloupe	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.38	e.e.meitav.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
79.178.9.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1476
212.179.46.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1028
185.26.180.150	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	274
46.19.86.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	274
37.26.148.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	88
77.126.238.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
85.250.135.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
176.12.145.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
149.88.74.246	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
95.220.87.38	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
154.100.173.32	Sudan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
213.151.37.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
187.175.83.100	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
37.26.147.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
91.180.73.215	Belgium	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
109.253.128.213	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
149.254.186.199	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
178.62.32.61	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
46.19.85.0	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
168.63.137.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
37.26.147.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
177.197.165.219	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
31.168.235.222	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.19.85.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
37.26.147.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
176.12.139.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
157.55.39.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.253.144.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
79.183.186.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
157.55.39.6	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
84.228.144.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
31.193.51.59	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
2.54.168.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
84.229.174.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
95.86.120.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
87.68.12.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
176.12.146.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.46.13.82	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
176.12.145.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
207.46.13.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
78.58.137.175	Lithuania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
80.246.133.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
213.57.105.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.181.209.196	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.209.196	Block	277
77.127.73.200	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
82.205.5.164	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
74.220.199.26	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
77.222.56.207	Russian Federation	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.177.125.222	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	2
212.16.233.141	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
77.127.170.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.52.159.237	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	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
5.29.14.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigato n.asp	Block	2
198.58.84.30	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
113.20.6.89	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
80.246.130.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/miktzoa/default.asp	None	1
84.228.63.247	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nahal/nahal.stm	Block	1
67.243.158.69	United States	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
188.138.17.205	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
128.72.140.209	Russian Federation	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
82.145.217.9	Europe	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-ar	Block	1
212.16.233.141	Germany	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
85.250.135.85	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
197.44.221.55	Egypt	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.15//80	Block	1
141.212.122.146	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
178.54.53.7	Ukraine	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
112.111.188.90	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp/trackback/	Block	1
79.181.209.196	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
198.58.84.30	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
141.212.122.146	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.108.167.17	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
77.127.170.100	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
182.118.53.252	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
113.20.6.89	Australia	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
74.220.199.26	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	1
84.228.63.247	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.228.63.247	Block	1
77.222.56.207	Russian Federation	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
188.120.148.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
46.5.0.145	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1