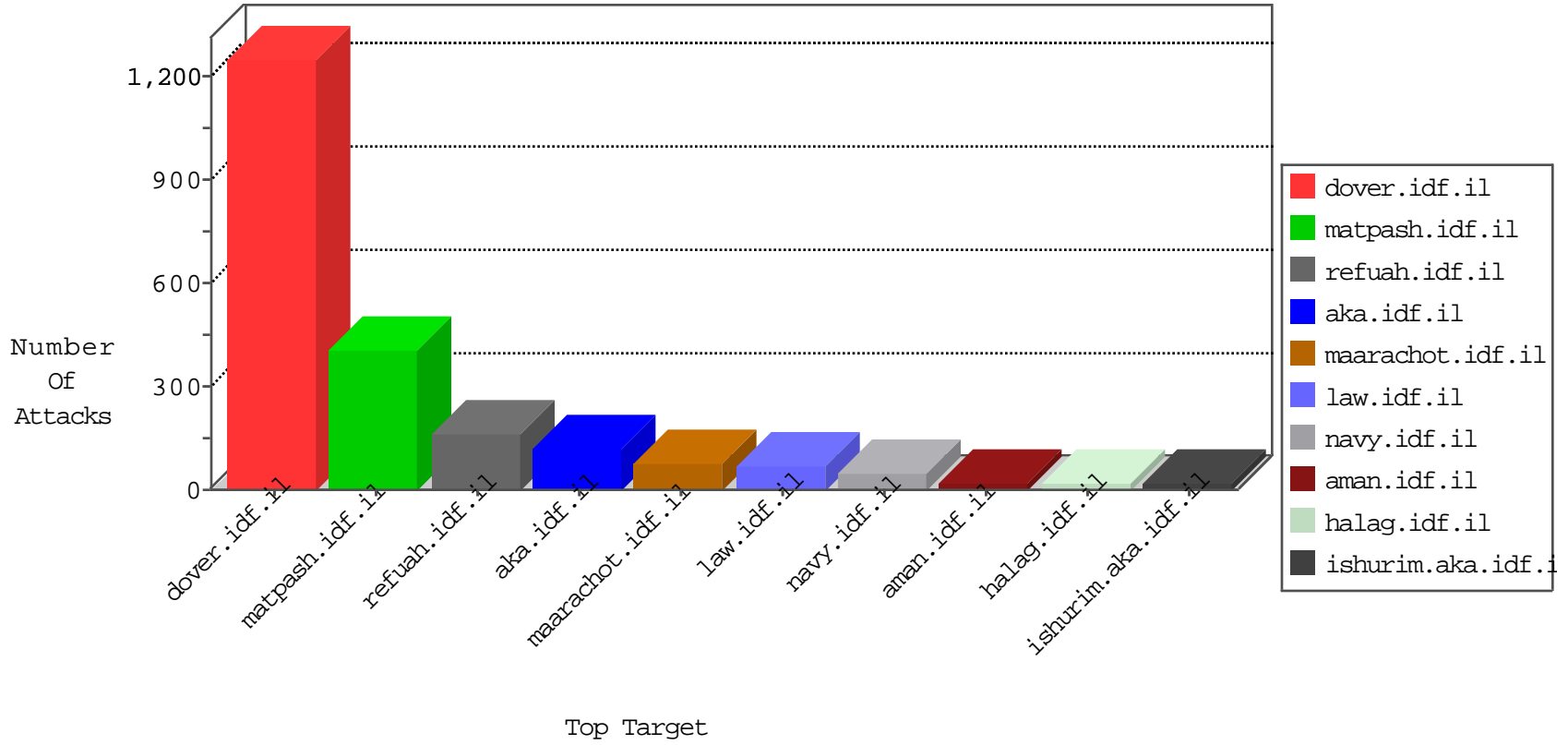
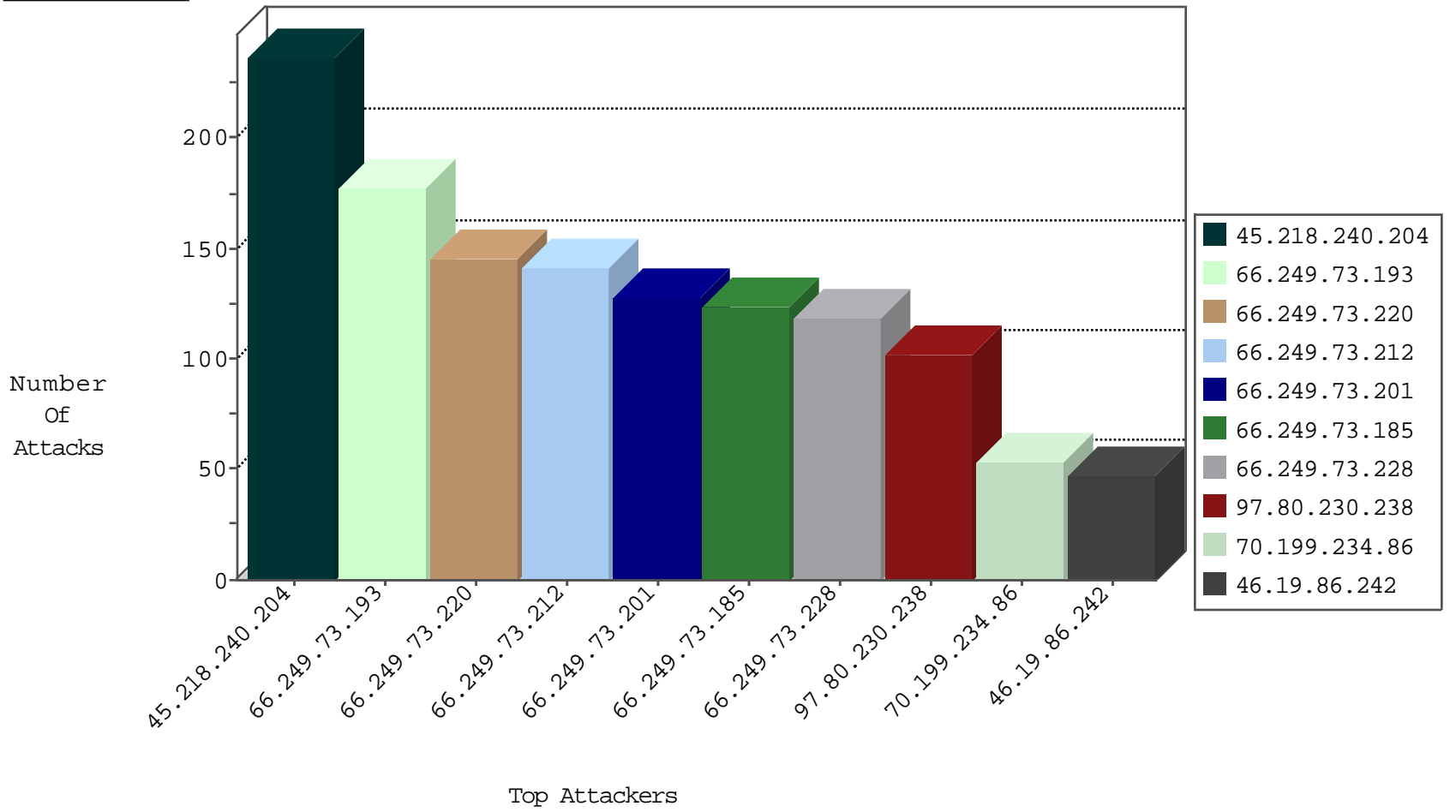


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.108	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	518
220.181.108.114	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	401
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	178
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	146
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	141
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	128
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	124
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	119
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	42
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	30
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	19
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	18
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	17
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	13
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	11
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.64.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.208	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.248	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.206	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.73.223	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
66.249.73.239	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
66.249.64.125	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.73.231	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	5
66.249.78.111	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	4
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.222	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	4
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	3
95.172.79.156	United Kingdom	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	3
66.249.64.196	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	3

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	25
64.79.144.10	United States	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	11
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2
109.67.10.30	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	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
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	6
150.108.68.29	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
91.148.168.184	Bulgaria	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS User-Agent used in Injection Attempts	3
91.148.168.184	Bulgaria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
27.123.168.210	Fiji	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
192.64.180.14	United States	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
27.123.168.210	Fiji	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
182.140.132.60	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
27.123.168.210	Fiji	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
182.140.132.60	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
27.123.168.210	Fiji	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
27.123.168.210	Fiji	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
69.12.92.160	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
27.123.168.210	Fiji	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
182.140.132.60	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
27.123.168.210	Fiji	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
182.140.132.60	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
27.123.168.210	Fiji	147.237.76.147	chimuch.aka.idf.il	ET SCAN Potential SSH Scan	1
182.140.132.60	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
27.123.168.210	Fiji	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
61.160.224.128	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
45.218.240.204		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	237
97.80.230.238	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	102
46.19.86.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
67.248.244.169	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
87.69.139.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
70.199.234.86	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
46.115.139.63	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
108.209.113.11	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
70.192.203.224	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
185.5.154.219	Saudi Arabia	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	12
31.203.133.228	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
109.253.139.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
70.199.234.86	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	10
70.199.234.86	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
176.12.147.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
91.148.168.184	Bulgaria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.253.144.50	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.151.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
70.199.234.86	United States	147.237.77.216	dover.idf.il		Bad TCP sequence	monitor	4
99.116.237.61	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
176.12.137.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.102.254.237	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.237.149.53	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
62.76.184.59	Russian Federation	147.237.0.15	kosher-kravi.idf.il	SAM rule	drop	drop	3
62.76.184.59	Russian Federation	147.237.72.166	aka.idf.il	SAM rule	drop	drop	3
62.76.184.59	Russian Federation	147.237.76.31	nakchal.idf.il	SAM rule	drop	drop	3
109.253.146.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
24.14.162.121	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
211.244.83.250	Korea, Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.23.227.223	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
198.58.103.36	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.142.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
117.78.13.29	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
185.5.154.219	Saudi Arabia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.145.208.219	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
198.58.103.115	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
125.209.235.170	Korea, Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
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	4
108.19.70.215	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
150.108.68.29	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluintemplates/inner.asp	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.241	Block	1
107.170.164.163	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
63.141.249.44	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-en/+navmenu.qc+	Block	1
150.108.68.29	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 150.108.68.29	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/580-he/sb_item_lvl	Block	1
1.10.248.61	Thailand	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/brothers/skira/default.asp	None	1
66.177.129.213	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/insignia/insignia.stm	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.65.123.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
150.108.68.29	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/9459.pdf&	Block	1
79.183.67.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
37.44.92.188	Belarus	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/brothers/faq/default.asp	None	1
113.162.71.107	Vietnam	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/brothers/home/default.asp	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
188.162.228.82	Russian Federation	147.237.72.166	aka.idf.il	Unknown HTTP Request Method COOK in URL www.aka.idf.il/brothers/skira/default.asp	Block	1
85.65.143.244	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
54.198.210.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
150.108.68.29	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1