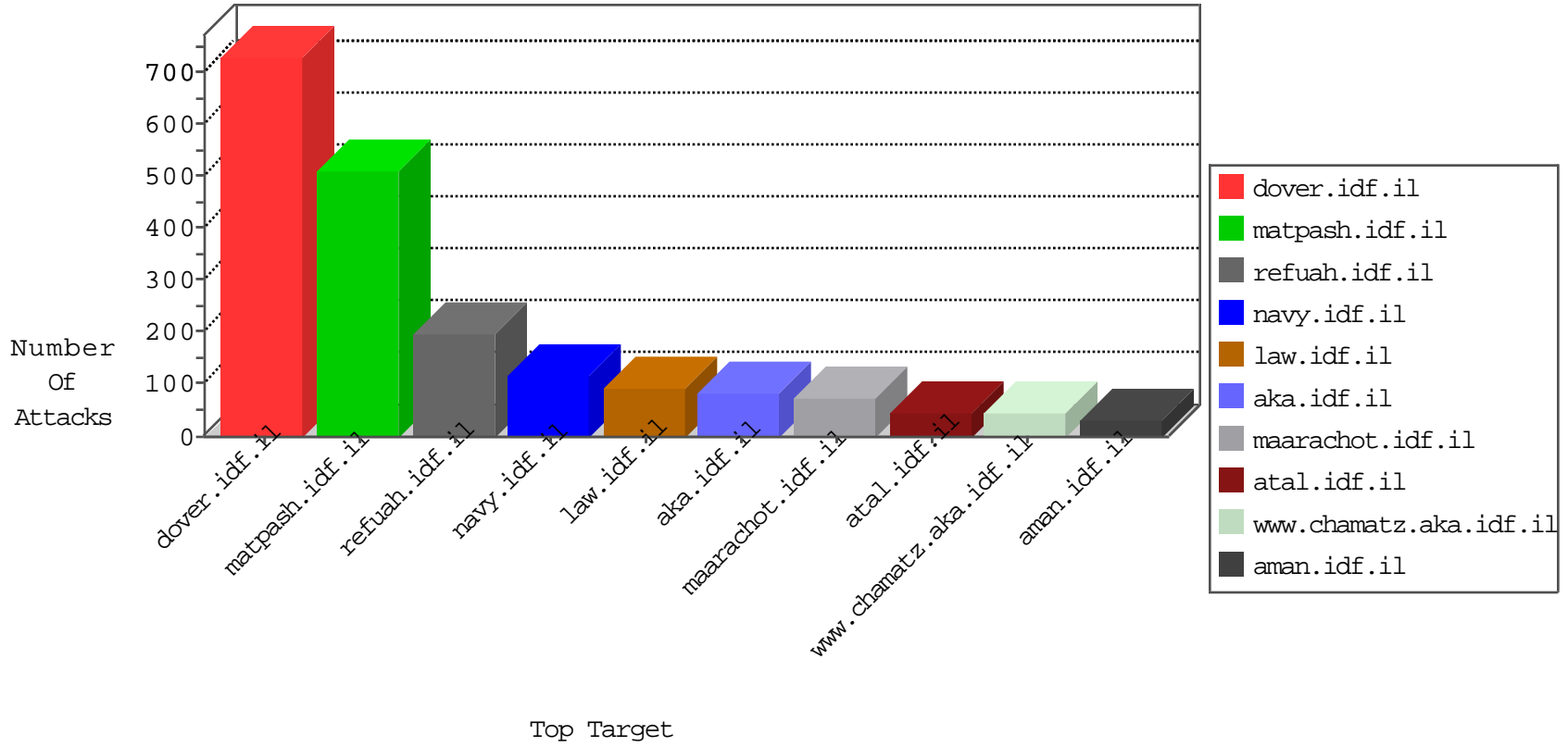
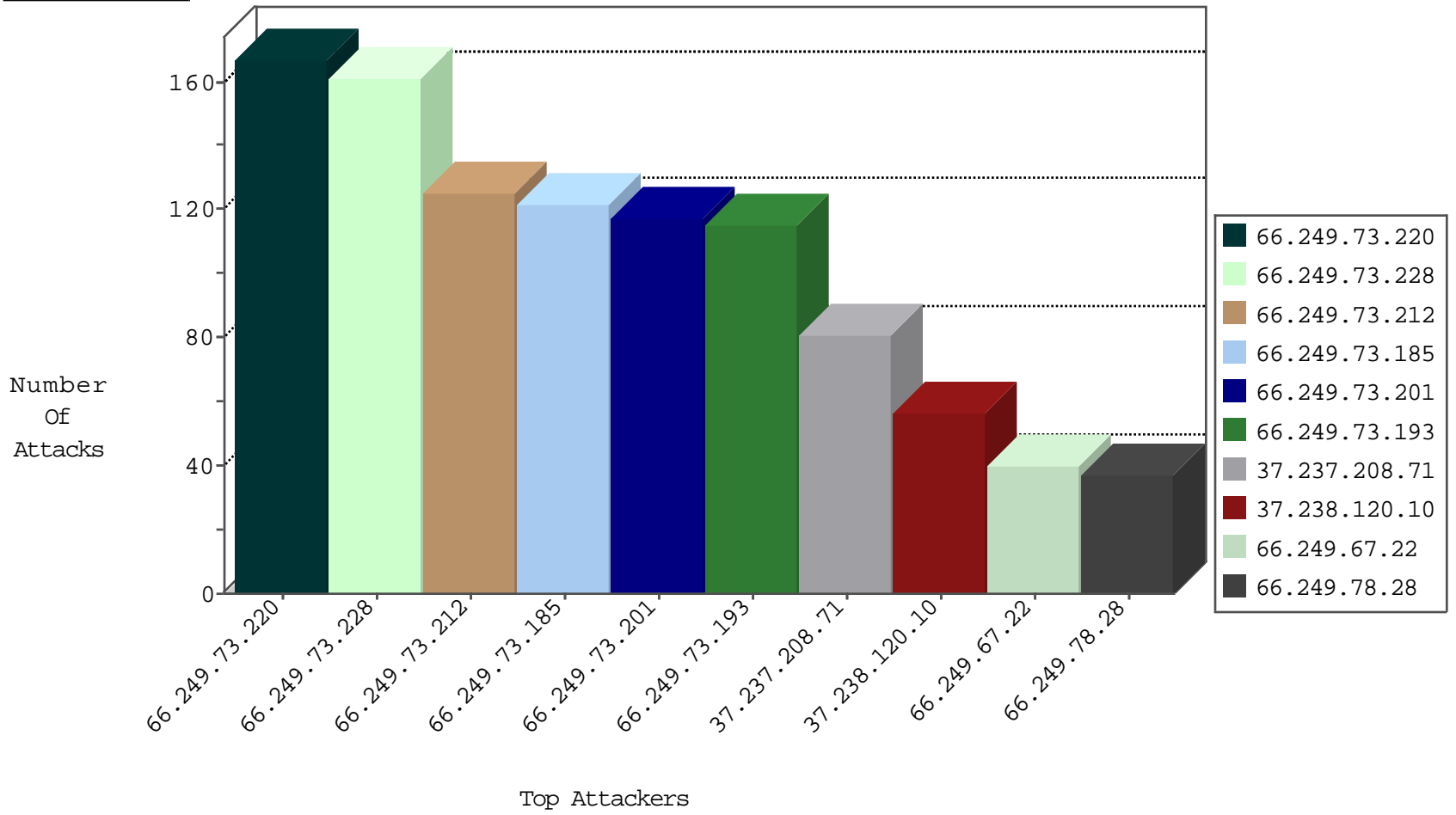




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.178	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3622
37.238.120.10	Iraq	147.237.77.176	matpash.idf.il	HTTP-POST-Segmented-DoS	dest-reset	432
24.112.131.185	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	332
84.110.8.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	170
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	167
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	161
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	121
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	118
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	117
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	115
37.238.120.10	Iraq	147.237.77.176	matpash.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	57
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	40
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	37
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	34
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	33
66.249.67.14	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	30
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	30
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	26
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	26
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	25
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.65.181	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	23
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	19
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.73.231	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	11
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.64.63	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.75.95	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.64.4	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.64.83	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5
66.249.64.38	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.64.79	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	4
66.249.65.185	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	4
66.249.64.8	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.238.120.10	Iraq	147.237.77.176	matpash.idf.il	8262: HTTP: Slowloris DoS Tool	Block	37
85.65.88.99	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.65.88.99	Israel	147.237.77.216	dover.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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	28
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	7
61.240.144.65	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
183.105.4.162	Korea, Republic of	147.237.0.35	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
23.238.137.197	United States	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
177.85.235.107	Brazil	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
23.238.137.197	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.245.99.48		147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
23.238.137.197	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
104.245.99.48		147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
23.238.137.197	United States	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
104.245.99.48		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 2048	1
91.224.132.118	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.17.72	Russian Federation	147.237.77.234	halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
69.12.92.160	United States	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
23.238.137.197	United States	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
177.85.235.107	Brazil	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
23.238.137.197	United States	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
175.143.109.18	Malaysia	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
23.238.137.197	United States	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
104.245.99.48		147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
23.238.137.197	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
104.245.99.48		147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 3072	1
99.244.135.30	Canada	147.237.76.30	himush.idf.il	ET SCAN NMAP -f -sS	1
193.107.17.72	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.176	test.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
37.237.208.71	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	81
46.19.85.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
41.176.195.42	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
213.151.32.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
24.112.131.185	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
75.110.253.228	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
176.12.146.106	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
208.69.40.107	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
149.147.45.132	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
69.167.57.80	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.86.196	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
62.76.184.59	Russian Federation	147.237.76.86	navy.idf.il	SAM rule	drop	drop	6
87.69.142.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.26.146.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
181.64.199.10	Peru	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.182.18.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.73.168	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	4
23.113.168.196	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
5.9.38.157	Germany	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
62.76.184.59	Russian Federation	147.237.76.42	refuah.idf.il	SAM rule	drop	drop	3
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
220.255.1.88	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.180.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.145.218.11	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.108.22.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
220.181.108.185	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
103.6.151.209	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.120.148.195	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
104.2.245.17	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
220.181.108.152	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.233.166	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
123.125.71.113	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
220.181.108.160	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
104.2.245.17	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
185.13.192.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	3
176.10.104.227	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.10.104.227	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
188.165.15.241	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.241	Block	2
63.141.249.44	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx	Block	1
206.253.226.14	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
109.253.142.27	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
176.10.104.227	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
112.104.85.148	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter in www.aka.idf.il/brothers/skira/default.asp	None	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=1e28e4c5kkkkkkk_1e28e4c5	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	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
37.215.11.42	Belarus	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/brothers/skira/default.asp	None	1
144.76.15.235	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
46.118.119.63	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
76.164.205.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1