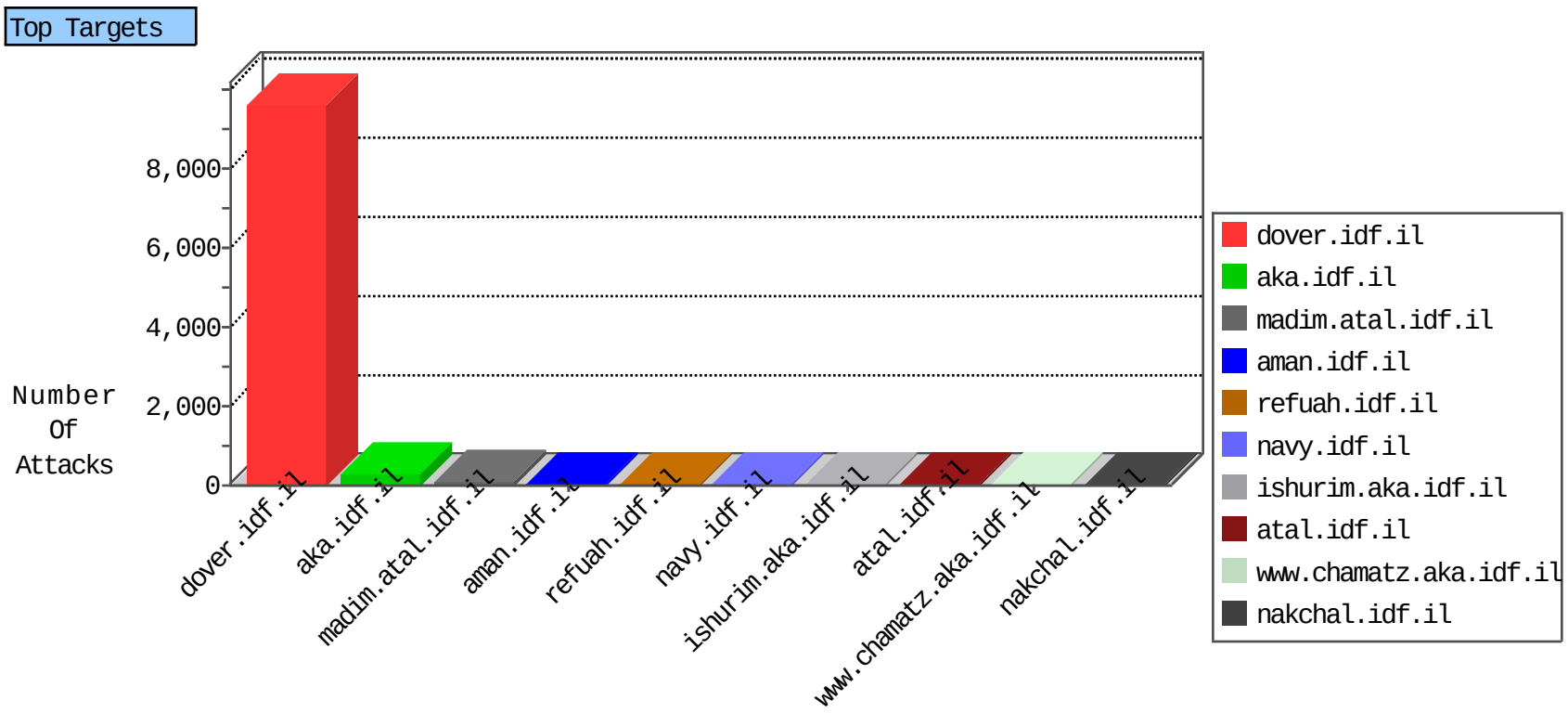
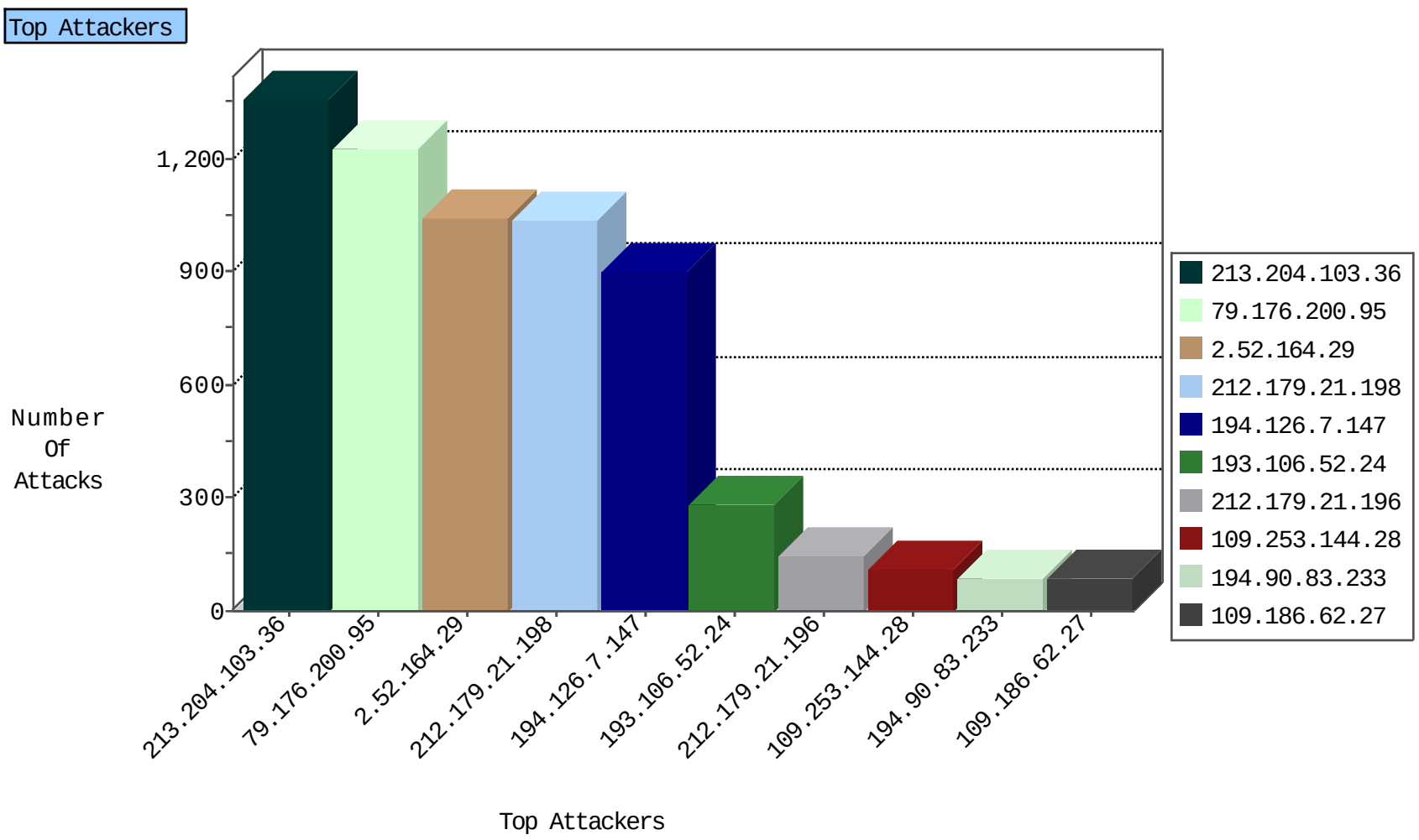
05-11-2015-15:03:05 to 05-11-2015-16:03:05

IDF Under Attack
05-11-2015-15:03:05





05-11-2015-15:03:05 to 05-11-2015-16:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.95.59.230	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2963
2.54.162.108	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	421
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	279
79.176.12.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	219
2.54.14.240	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
109.186.184.234	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	68
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
194.90.83.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
193.43.244.72	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
64.94.179.36	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
159.104.163.18	United Kingdom	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
82.231.245.119	France	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
64.94.179.44	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
64.94.179.12	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
111.202.66.66	China	147.237.76.39	mobile.meitav.idf.il	L4 Source or Dest Port Zero	drop	1
64.94.179.56	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
95.172.79.236	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
64.94.179.28	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
149.88.23.121	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.162.108	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
95.172.79.244	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

05-11-2015-15:03:05 to 05-11-2015-16:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.179.132.202	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.121.86.118	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
168.1.79.114	Switzerland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	2
81.218.175.39	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.166.144.142	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
84.108.84.250	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
147.236.38.135	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
61.47.69.84	Thailand	147.237.77.170	maarachot.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
85.25.43.94	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1

05-11-2015-15:03:05 to 05-11-2015-16:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
62.90.220.166	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.130	China	147.237.77.205	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.69.94.13	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.179.21.198	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.16.232.231	India	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.45.192.252	Seychelles	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.164.29	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.11	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.7.84	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.79.31	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.65	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.89.137.3	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.130	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.179.21.196	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.162.127	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.146.151	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.155.56	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.187.19	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

05-11-2015-15:03:05 to 05-11-2015-16:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1359
79.176.200.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1227
2.52.164.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1035
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	938
194.126.7.147	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	902
193.106.52.24	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	285
212.179.21.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	147
109.186.62.27	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	84
194.90.83.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
128.139.251.9	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	66
85.65.84.220	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
80.246.133.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
82.166.126.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
2.71.45.215	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
85.250.30.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
205.200.199.36	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
37.26.147.154	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
109.253.145.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
5.102.254.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
2.54.40.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
98.193.63.151	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
109.253.137.107	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
41.221.97.74	Malawi	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
138.246.2.11	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
92.243.181.74	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
132.74.215.237	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
46.19.86.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
212.179.21.198	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	29
212.179.21.198	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	29
212.179.21.198	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	29
46.19.85.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
62.20.57.5	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
109.253.138.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
80.246.133.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
2.54.162.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
46.60.76.196	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
2.52.162.75	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	22
2.54.161.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
2.52.162.75	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	22
213.57.219.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
2.52.162.75	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	22
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
79.179.141.115	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
82.139.112.63	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
79.182.96.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.144.28	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.144.28	Block	108
46.117.128.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	11
149.88.107.86	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
46.116.90.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
84.94.170.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
62.219.185.242	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	3
185.32.177.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
185.32.178.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	2
79.179.141.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.250.86.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.223.27.26	United States	147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/../images/shared/home.png	Block	1
80.179.163.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
66.249.73.213	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.73.213	Block	1
109.253.129.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
82.145.218.232	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1365-he/refuah.aspx	Block	1
188.165.15.138	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.64.187	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
89.139.10.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
80.246.130.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
82.166.144.142	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
66.249.79.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1437-he/refuah.aspx	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.20	United States	147.237.72.166	aka.idf.il	Unknown Parameter 177afae0 in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.65.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/×©×§×•×¤×™×ª 9	Block	1
37.26.147.181	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
90.149.166.227	Norway	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
81.218.33.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
185.32.178.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.121.132.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
132.74.215.237	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 132.74.215.237	Block	1
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	1
176.12.137.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
37.26.147.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.82.58	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
188.138.17.205	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
50.243.68.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/navy/service.stm	Block	1
84.228.32.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
176.12.150.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.205	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.73.205	Block	1
37.142.207.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
109.64.81.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1