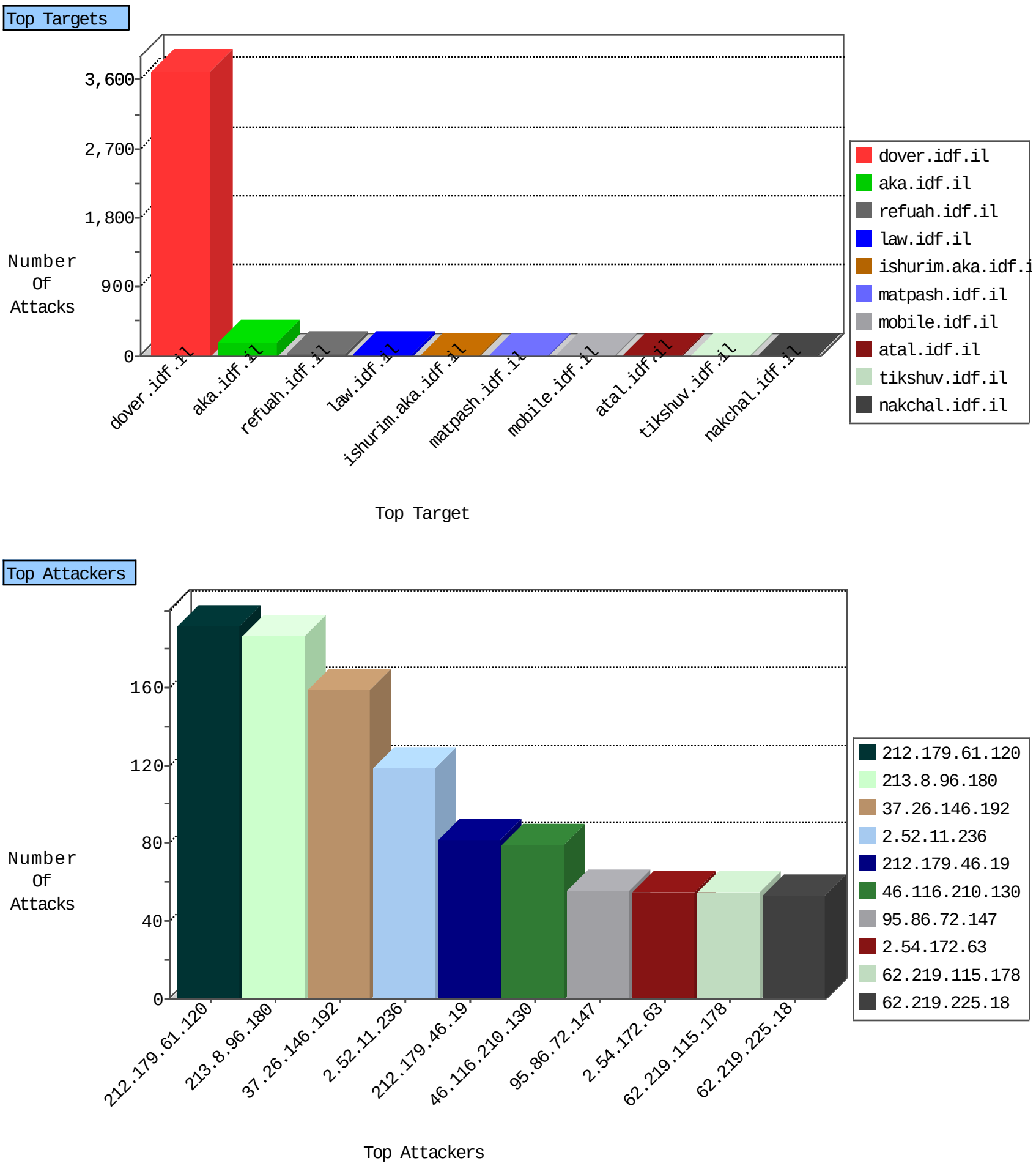
05-10-2015-09:03:04 to 05-10-2015-10:03:04

IDF Under Attack
05-10-2015-09:03:04



05-10-2015-09:03:04 to 05-10-2015-10:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
149.78.37.250	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
80.246.135.51	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
80.246.137.62	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
213.8.96.180	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
109.65.21.13	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
41.209.76.238	Sudan	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
2.54.30.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
37.26.147.200	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.118.64.213	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	2
2.52.10.108	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
202.168.106.96	Australia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
62.0.7.122	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
79.183.26.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.74.96.29	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
46.121.62.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1
82.80.180.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.20.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.69	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.179.61.120	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
89.139.162.27	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
182.187.66.78	Pakistan	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.246.138.94	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-10-2015-09:03:04 to 05-10-2015-10:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.100	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	2
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.201	e.atal.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
71.6.167.142	United States	147.237.76.38	e.e.meitav.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
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.117	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.94.203.62	Israel	147.237.77.216	dover.idf.il	C10000004: HTTP: options method (Microsoft)	Block	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1

05-10-2015-09:03:04 to 05-10-2015-10:03:04

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	2
2.52.43.125	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.83.139.68	France	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
109.253.147.57	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.138.195	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.62.133	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.251.242	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.229.182	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.82	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.65.104	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.98.3	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.108.72	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.242.201	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.7.131	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.65.76	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.67	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

05-10-2015-09:03:04 to 05-10-2015-10:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	190
213.8.96.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	162
37.26.146.192	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	159
2.52.11.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	119
212.179.46.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
46.116.210.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	79
95.86.72.147	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
62.219.115.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
2.54.172.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
62.219.225.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
31.168.99.83	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
178.80.66.184	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
176.12.137.94	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
37.26.147.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
195.160.240.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
46.19.86.222	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
46.19.85.202	Israel	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	33
80.74.101.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
31.168.79.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
176.12.151.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
79.180.55.239	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
80.179.223.31	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
104.48.69.214		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
2.54.30.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
148.177.129.213	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
2.54.150.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
213.8.96.180	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	18
37.140.141.37	Russian Federation	147.237.77.74	law.idf.il	SAM rule	drop	drop	18
212.199.224.24	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
84.108.87.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
85.250.12.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
80.230.28.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
212.25.84.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
89.138.192.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
81.218.251.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
46.120.160.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
37.26.147.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
138.134.192.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
93.172.14.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
62.0.7.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
2.54.151.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
195.242.218.133	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	6
46.19.86.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
46.19.86.48	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
212.179.246.75	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
77.125.7.214	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.150.66.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
37.26.147.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.177.154.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
62.90.35.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
185.32.176.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
84.94.111.203	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
5.144.61.172	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
212.199.58.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
74.82.47.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.67.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71555-he/maarachot.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.37.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.156.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
217.66.237.180	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-ar	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1349-he/refuah.aspx	Block	1
46.121.108.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
31.186.228.58	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.226.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
212.199.224.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.91	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71850-he/maarachot.aspx	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	1
81.218.56.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.187.164	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.79.113	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/938-he/atal.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mp/	Block	1
89.139.4.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
213.8.38.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
77.237.138.202	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	1
46.19.86.138	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
82.80.196.44	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
2.54.39.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
212.179.21.197	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.81.222	Israel	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../favicon.ico	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	1
62.90.144.182	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
37.26.147.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
94.159.165.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.8.62.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1

05-10-2015-09:03:04 to 05-10-2015-10:03:04