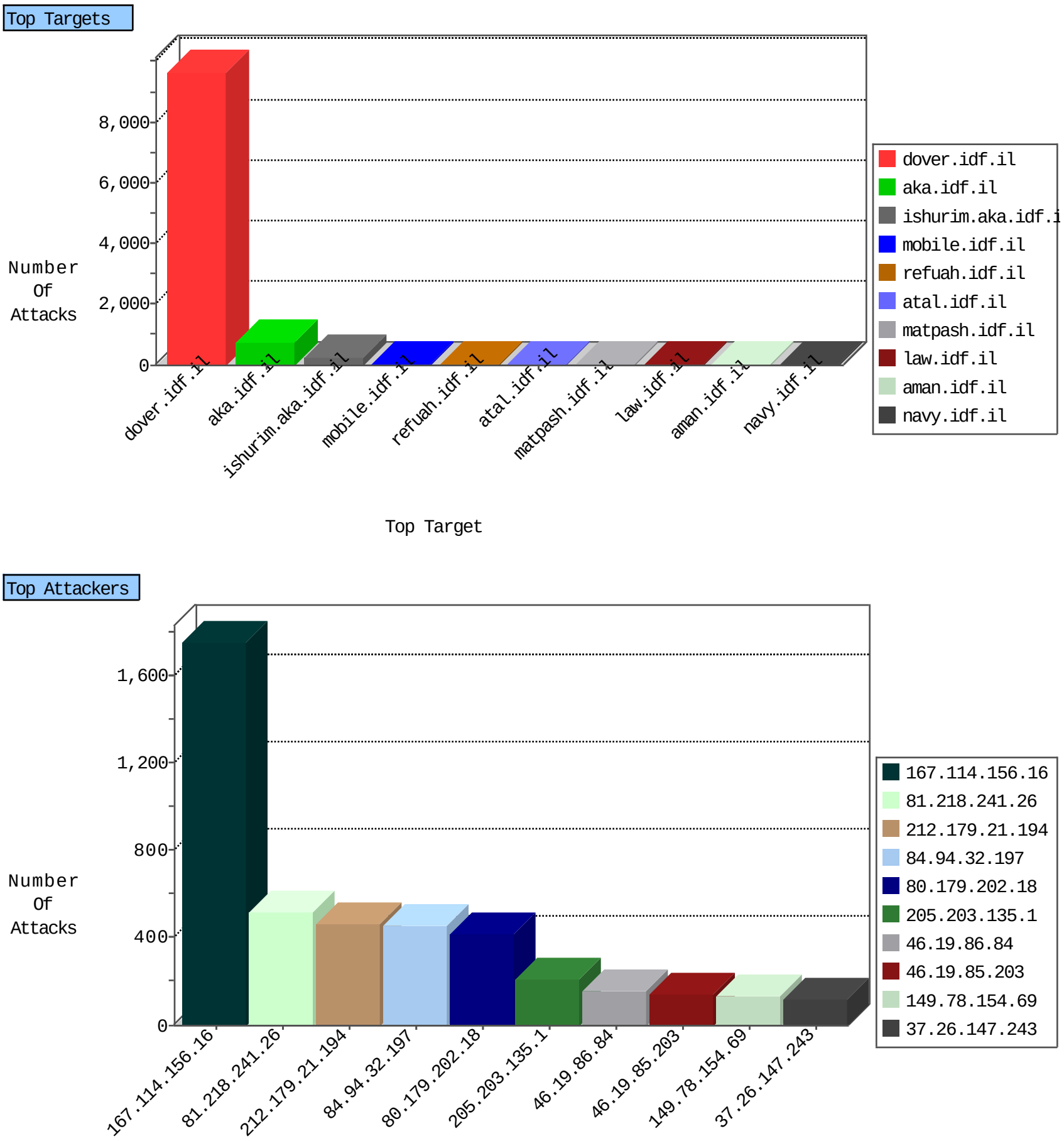
11-02-2015-10:04:05 to 11-02-2015-11:04:05

IDF Under Attack Daily Report



11-02-2015-10:04:05 to 11-02-2015-11:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2842
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	172
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
2.54.157.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
2.54.31.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
2.54.31.81	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
192.115.177.202	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
46.19.85.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.13.14.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
37.26.147.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.13.13.177	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
2.54.148.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.86.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
77.127.197.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
192.114.2.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
31.168.228.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
2.54.27.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.64.102.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.65.75.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.16.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
147.236.38.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.67.154.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
149.78.7.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
78.40.176.183	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.146.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
95.86.80.234	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
176.12.160.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.4.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
95.86.80.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.52.175.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.151.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
146.185.239.100	Russian Federation	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
109.64.190.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.12.137.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
109.65.75.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.64.190.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.52.18.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.12.144.147	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
109.65.59.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
110.77.212.85	Thailand	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
46.19.86.147	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-02-2015-10:04:05 to 11-02-2015-11:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.68.49	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
80.246.139.60	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	3
79.177.202.171	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.66.133.120	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
82.80.33.42	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-02-2015-10:04:05 to 11-02-2015-11:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.188.81	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	34
176.13.4.75	147.237.0.19	Israel	madim.atal.idf.il	GPL SCAN myscan	2
66.249.67.34	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
176.13.4.75	147.237.0.19	Israel	madim.atal.idf.il	INDICATOR-SCAN myscan	2
2.54.27.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.106.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.206.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.131.179.3	147.237.76.31	Mexico	nakchal.idf.il	ET SCAN NMAP -f -sS	1
77.248.67.138	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
64.46.23.242	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.5.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.184.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.147.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.227.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
110.172.17.199	147.237.8.46	India	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.186.41.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.158.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.84.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.131.179.3	147.237.76.31	Mexico	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
79.180.195.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.106.226.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.14.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.147.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
60.10.71.39	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
176.13.2.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.138.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
110.172.17.199	147.237.8.28	India	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
84.111.157.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-02-2015-10:04:05 to 11-02-2015-11:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.241.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	512
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	456
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	456
80.179.202.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	418
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	212
46.19.86.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	135
92.40.249.57	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
37.26.147.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
46.19.85.203	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	96
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
123.103.8.48	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
95.86.80.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
5.29.76.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
37.26.146.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
37.26.148.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
46.19.86.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
185.22.32.10	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
2.52.20.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
62.219.50.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
79.178.154.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
37.26.146.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
176.12.139.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
212.179.4.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
2.52.141.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
109.65.161.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
213.57.128.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
109.65.75.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
37.26.146.215	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
2.54.176.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
17.142.152.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.85.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
80.149.240.82	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
109.67.174.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.210.203.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.83.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.85.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
2.54.148.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.13.8.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.107.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	5
2.54.0.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
176.12.137.173	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	4
5.22.129.146	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	4
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
213.151.48.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/ain/giyus	Block	2
81.218.44.254	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	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
176.13.13.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.154.168.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
213.151.48.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.151.48.6	Block	2
46.19.86.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.147.247	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
2.54.31.40	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
79.177.202.171	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/6/size338x0/1596.jpg	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.91.30	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.52.18.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
37.26.148.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.169.226	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.41.121	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.102.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
109.66.8.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.116.80.231	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
81.218.124.66	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
77.125.111.200	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
176.13.15.90	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.142.254.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.110.83.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
2.54.56.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
132.71.80.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	1
46.116.80.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
81.218.241.26	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/images/shared/mainbackbig.jpg	Block	1
31.168.170.54	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
2.54.4.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.111.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/ajax/updatestatus.php	Block	1
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.55.148	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.133.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.135.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1