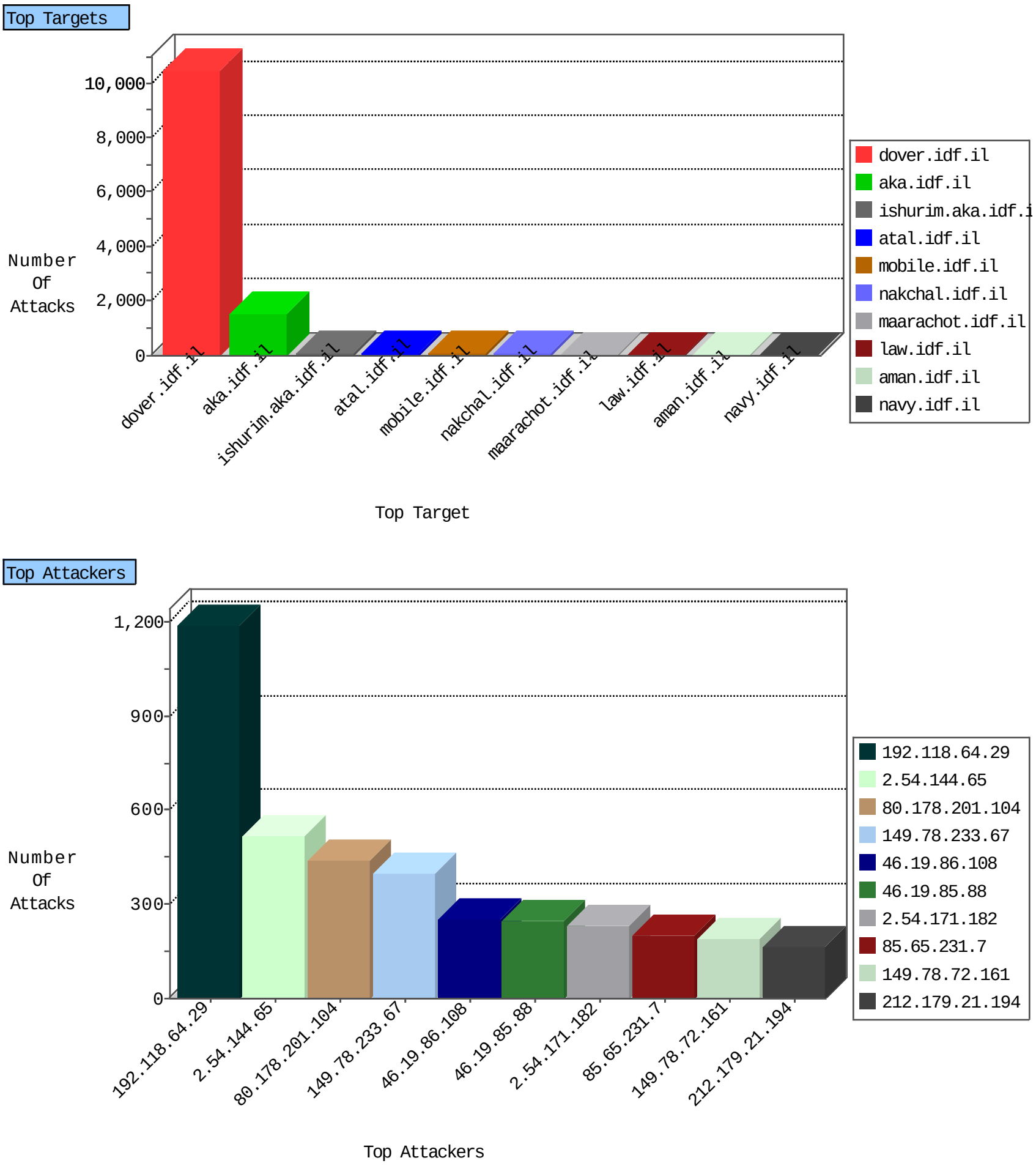
10-18-2015-15:04:00 to 10-18-2015-16:04:00

IDF Under Attack Daily Report



10-18-2015-15:04:00 to 10-18-2015-16:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.226	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2974
46.116.145.76	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2922
208.115.111.73	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2508
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	992
185.32.179.186	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	154
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
192.114.23.209	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	32
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	31
31.154.24.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
87.68.40.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
31.154.92.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
2.54.142.116	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
37.26.148.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
31.168.133.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
79.181.27.147	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
46.19.86.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
80.178.201.104	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
46.19.86.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.19.86.53	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
176.12.138.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
2.54.142.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
192.168.1.4		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
84.111.6.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.180.65.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
84.111.6.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.180.65.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.12.148.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.25.83.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
109.64.198.69	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
176.12.145.21	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.19.85.230	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
2.54.144.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.85.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.86.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
87.68.40.73	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
79.180.181.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
77.126.128.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
192.118.64.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
84.95.131.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
84.108.33.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
212.150.222.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.94.49.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.12.145.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.166.28.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
149.78.72.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
91.231.193.150	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.146.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.120.198.159	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
82.166.22.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5

10-18-2015-15:04:00 to 10-18-2015-16:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.90.134.253	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.181.58.56	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

10-18-2015-15:04:00 to 10-18-2015-16:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
201.249.199.91	147.237.0.19	Venezuela	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.128.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.69.105.238	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.160.198.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.150.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
74.82.194.10	147.237.72.156	Canada	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.249.199.91	147.237.0.34	Venezuela	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.117.98.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.91.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.42.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.137.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.189.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.249.199.91	147.237.0.200	Venezuela	m4u.idf.il	ET SCAN Potential SSH Scan	1

10-18-2015-15:04:00 to 10-18-2015-16:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.118.64.29	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1177
2.54.144.65	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	501
149.78.233.67	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	397
46.19.85.88	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	248
46.19.86.108	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	248
2.54.171.182	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	232
85.65.231.7	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	201
149.78.72.161	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	187
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	160
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	134
185.51.213.54	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	126
46.19.85.3	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	108
185.27.105.66	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	104
149.78.180.82	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
85.64.213.163	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	87
46.19.86.23	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	87
46.19.86.230	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	79
176.13.20.217	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
95.160.72.75	Poland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	69
213.151.47.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	61
185.71.143.100	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
46.19.85.175	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
84.108.237.149	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.85.230	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
2.54.149.126	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
62.219.225.85	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
82.166.22.9	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
2.54.142.116	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
80.178.201.104	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
41.36.250.217	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
212.199.195.61	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
92.241.33.203	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
66.249.78.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
62.219.121.10	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
66.249.78.159	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
66.249.78.166	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
66.249.88.91	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
192.118.78.199	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.201.104	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	399
93.172.7.22	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 93.172.7.22	Block	143
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	78
94.159.168.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	26
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
85.64.213.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
84.108.17.71	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
37.26.148.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
183.57.154.56	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/webresource.axd%3fd	Block	13
79.181.121.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
121.26.192.114	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	13
66.249.81.141	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
46.19.85.170	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	13
213.57.231.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	13
84.228.118.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	13
31.13.102.119	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
168.235.194.250	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clie×²Ö³Ö´	Block	13
81.218.203.167	Israel	147.237.72.166	aka.idf.il	Too Many Cookies in a Request - 103 cookies	Block	13
79.176.227.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
109.66.134.39	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	13
46.72.212.254	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
89.139.8.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter mouduletogo in aka.idf.il/main/giyus/login.aspx	None	13
84.108.17.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
37.26.148.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
185.32.179.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
121.26.192.114	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/utility/convert/index.php	Block	13
79.182.176.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
2.54.164.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
95.86.68.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
66.249.93.153	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
46.19.86.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
213.151.54.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	13
85.64.72.212	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
31.168.230.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
176.12.137.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	13
79.176.227.120	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	13
109.67.173.250	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	13
46.210.252.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	13
84.108.33.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
37.142.209.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
207.46.13.88	United States	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	13
5.29.167.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sahar	Block	13
147.235.185.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/haredim/scriptresource.axd	None	13
79.183.24.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
109.64.180.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
46.19.86.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
213.151.54.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
31.210.186.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	13
176.13.2.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13