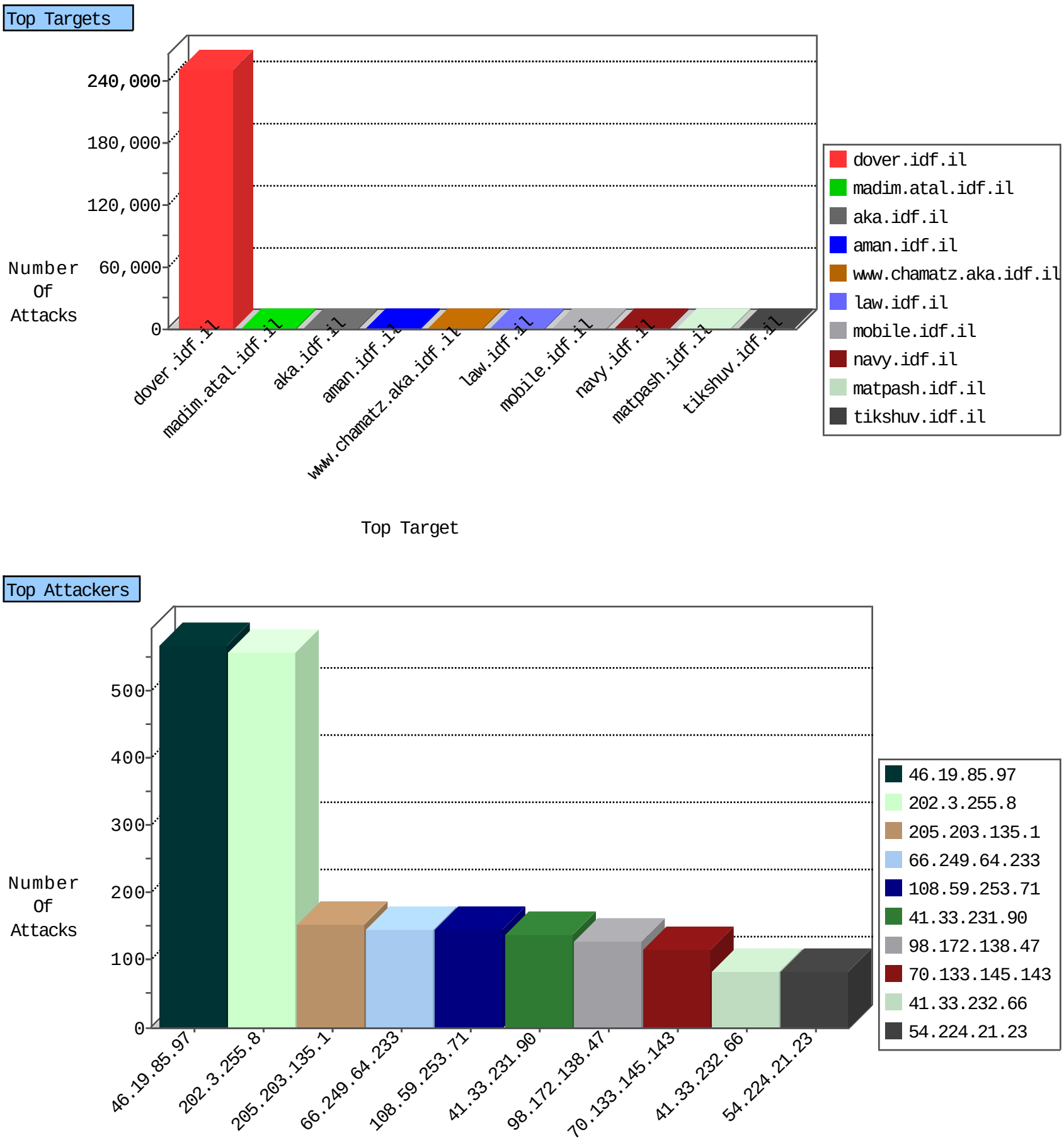
11-18-2015-00:04:05 to 11-18-2015-01:04:05

IDF Under Attack
Daily Report



11-18-2015-00:04:05 to 11-18-2015-01:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.37	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6762
14.100.62.86	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3193
126.141.58.120	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2729
41.105.45.154	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	604
14.64.182.119	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	231
126.218.73.116	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	197
204.93.154.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	175
24.202.74.40	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	169
190.247.176.93	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	108
179.231.143.106	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	53
126.50.124.104	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	11
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
77.210.187.94	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
46.19.86.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.251.218.46	Finland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
31.211.235.102	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
31.208.62.41	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
65.218.74.68	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
88.203.153.27	Bulgaria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.111.78.38	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.31.207.112	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
126.203.116.90	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
31.209.35.31	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
116.200.3.109	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.30.187.3	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
195.1.60.57	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.166.5	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
100.42.166.14	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
79.160.150.60	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.152.68.88	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.53.78.98	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
59.164.232.79	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.229.209.23	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
222.119.146.111	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.200.28.60	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
91.190.9.65	Switzerland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
211.223.66.68	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.84.242.54	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
134.255.78.36	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.241.72.90	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
125.154.130.75	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
31.29.117.68	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.252.204.102	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.187.100	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.105.194.114	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
84.210.80.83	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.68.246.122	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-18-2015-00:04:05 to 11-18-2015-01:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.105.45.154	Algeria	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

11-18-2015-00:04:05 to 11-18-2015-01:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	522
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.65.248	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
64.15.1.55	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.203.99.38	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.102.88	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.62.81	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.223.68.31	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.136	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
140.170.18.37	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.175.189.102	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.151.109	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.221.24	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
58.83.10.67	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
68.168.137.2	147.237.76.147	Canada	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
136.228.201.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.165.13	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
205.175.168.51	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.13.38	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.26.51	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.86.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
136.228.186.1	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.159.75	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
68.168.137.2	147.237.8.28	Canada	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
110.232.171.72	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.0.81	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
45.127.207.216	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
199.26.112.15	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.79.115	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.133.57	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
68.168.137.2	147.237.0.19	Canada	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
148.178.218.77	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.220.15.199	147.237.77.243	Germany	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
198.205.75.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.134.42	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.234.105	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.145.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.64.233	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
148.105.89.15	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.151.69.117	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.41.65	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.88.92	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.238.12	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.148.78.98	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.231.88	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.162.23	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.10.45	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.181.123	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.96.60	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
207.189.8.126	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-18-2015-00:04:05 to 11-18-2015-01:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	146
98.172.138.47	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
70.133.145.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	107
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
188.50.171.253	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
71.234.124.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
78.96.141.161	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
71.125.29.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
41.105.45.154	Algeria	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.64.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
86.3.130.26	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	30
189.96.206.59	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
99.238.32.134	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	21
104.131.246.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
79.178.133.18	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
79.178.133.18	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
178.63.165.187	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.105.45.154	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
40.77.167.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
90.215.64.78	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
100.127.128.144		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
100.100.104.89		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
100.100.106.6		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.109.184.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
23.227.160.116	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
95.187.155.35	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.106.6		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
107.170.61.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
104.131.197.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

11-18-2015-00:04:05 to 11-18-2015-01:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.97	Block	301
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	159
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.97	Block	72
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	8
46.121.200.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.166.22.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.212.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
47.60.43.215	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.64.183.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.121.206.239	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
5.28.166.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.108.150.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/3467.jpg	Block	1
176.13.19.251	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 119 cookies	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
47.60.43.215	Spain	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
23.227.160.116	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
89.138.166.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
185.28.193.95	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
77.125.91.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
47.60.43.215	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
31.154.94.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.227.191.53		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/transportation.asp	Block	1
46.19.85.147	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.48	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/</font	Block	1
2.54.25.46	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3470.jpg	Block	1
149.88.66.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/tmuna	Block	1

11-18-2015-00:04:05 to 11-18-2015-01:04:05