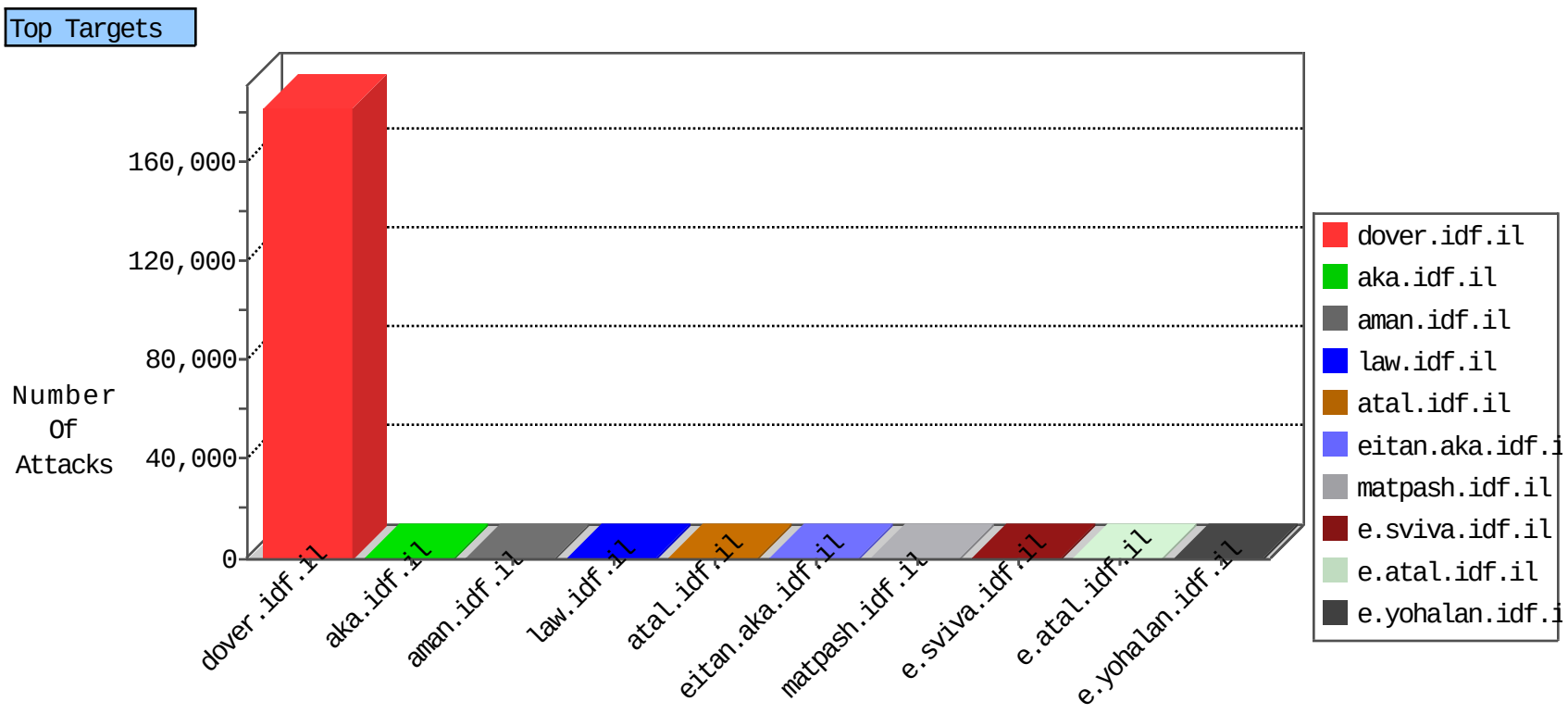
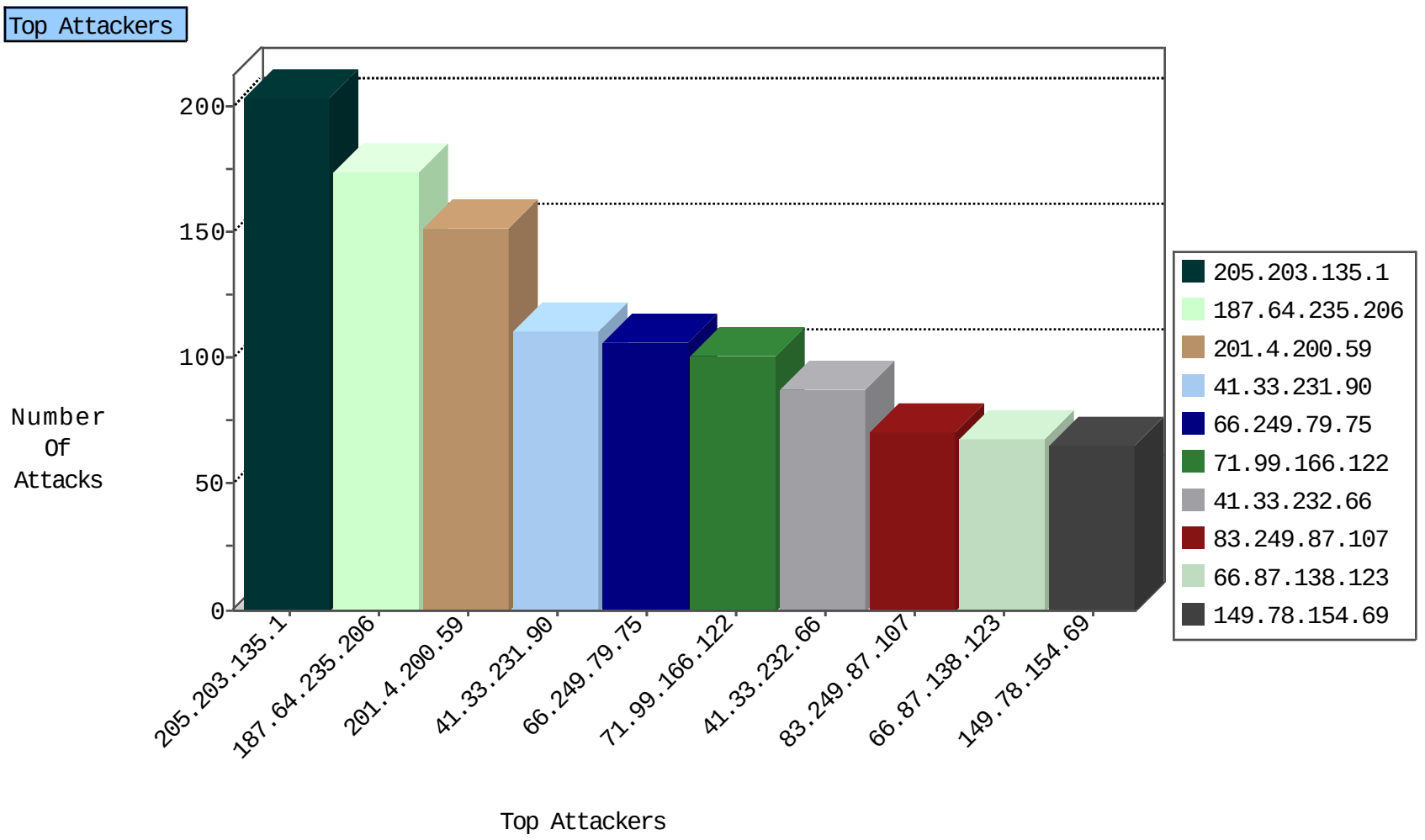
11-16-2015-02:04:08 to 11-16-2015-03:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-16-2015-02:04:08 to 11-16-2015-03:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.79.127	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6405
171.207.85.106	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3308
79.150.117.127	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2990
116.120.167.8	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2989
133.46.131.111	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2930
189.49.99.85	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2689
70.81.74.42	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2564
120.184.17.45	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2539
66.249.78.254	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1203
147.110.51.84	South Africa	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	448
187.26.55.69	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	352
24.230.107.61	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	302
64.122.81.33	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	274
59.10.117.110	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	172
126.78.40.46	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	147
222.99.226.36	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	105
219.139.97.28	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	97
61.53.162.26	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	84
190.255.212.25	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	82
133.14.90.97	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	81
112.208.192.160	Philippines	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	81
189.174.140.12	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	59
182.115.90.63	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	59
171.249.40.56	Vietnam	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	52
47.63.131.19	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	43
168.103.225.9	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30
117.214.234.124	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20
164.159.99.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
220.181.108.183	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	4
180.69.255.58	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
93.152.218.15	Bulgaria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
83.168.77.101	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
134.228.173.106	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
207.177.73.35	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
95.87.136.120	Slovenia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
183.156.5.109	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
38.69.37.19	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.160.80.17	Croatia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.29.110.112	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.186.24	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.199.4	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
193.77.91.55	Slovenia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.80.114	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.160.83.64	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.221.44.89	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.12.242.29	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.56.232.117	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
116.200.31.67	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.178.215.118	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-16-2015-02:04:08 to 11-16-2015-03:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	5
188.165.15.233	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	3
188.165.15.202	France	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.176	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.233	France	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-16-2015-02:04:08 to 11-16-2015-03:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
157.231.192.6	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
37.143.82.50	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
209.205.203.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
116.199.135.82	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.101.121	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.160.155	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
134.209.105.95	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.43.27	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
23.227.196.29	147.237.8.24	United States	e.lifestyle.idf	ET SCAN NMAP -sS window 2048	1
207.22.208.61	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
113.22.227.42	147.237.8.46	Vietnam	e.chinuch.idf.i	ET SCAN NMAP -f -sS	1
176.47.38.67	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.108.137.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
134.172.42.71	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
23.102.186.35	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
204.236.1.108	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
103.35.151.192	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
148.178.223.70	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.43.98	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.218.212.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.168.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.187.229.68	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
97.93.115.153	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
143.135.249.36	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.10.74.198	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
64.112.134.19	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.97.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.97.134.48	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.230.98.25	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.29.109	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.236.47	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.96.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.16.59	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.159.10	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.83.73	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.36.13	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.128.55	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.114.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
62.122.37.108	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
139.167.52.1	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.107.17.72	147.237.0.34	Seychelles	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
94.130.180.86	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.232.76.124	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.67	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
128.168.193.114	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.164.116	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
189.254.90.133	147.237.77.227	Mexico	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
94.130.18.59	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-16-2015-02:04:08 to 11-16-2015-03:04:08

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	204
187.64.235.206	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	174
201.4.200.59	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	152
71.99.166.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
83.249.87.107	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
66.87.138.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
71.92.79.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
107.23.6.162	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
92.29.135.21	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
66.249.79.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
52.25.108.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	33
157.55.39.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
2.54.55.198	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.65.10.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
109.65.10.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
128.242.249.10	United States	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
157.55.39.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	21
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
37.187.129.166	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.79.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
157.55.39.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
88.198.25.217	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.79.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
157.55.39.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.13.7.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
204.93.154.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
107.170.63.50	United States	147.237.77.216	dover.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
142.161.52.58	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
50.39.100.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11

11-16-2015-02:04:08 to 11-16-2015-03:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.97.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.172.50.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
31.193.51.80	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.143	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.69.8	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
79.183.178.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$txtPasswordRepeat in www.aka.idf.il/main/giyus/faq.aspx	None	1
40.77.167.30	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
66.249.73.238	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/modiin/maslul.aspx	Block	1
46.19.86.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
74.111.230.228	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/src="http:/www.youtube.com/v/0mwqtcld1fe	Block	1
104.128.144.131	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
79.176.59.65	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
24.230.107.61	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.85	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9589-he/refuah.aspx	Block	1

11-16-2015-02:04:08 to 11-16-2015-03:04:08