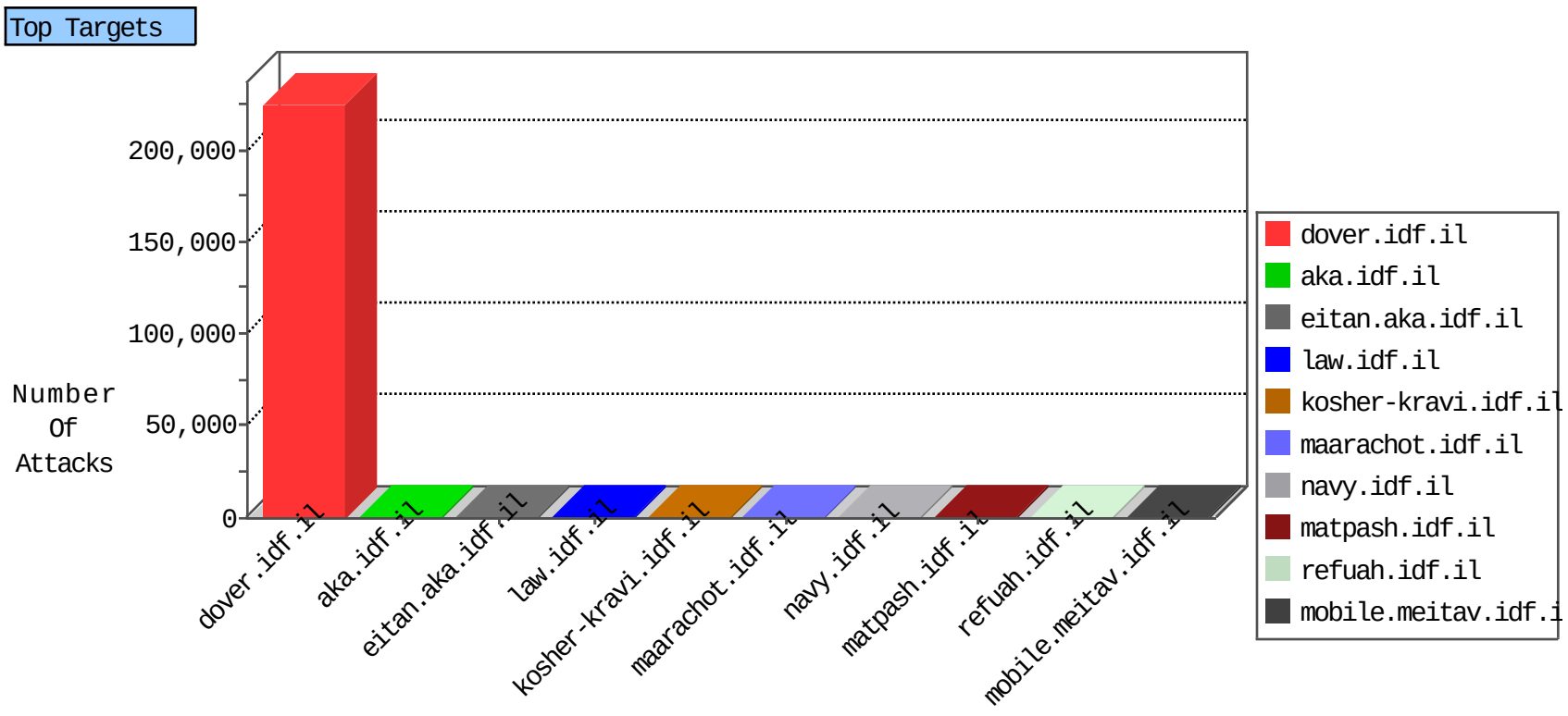
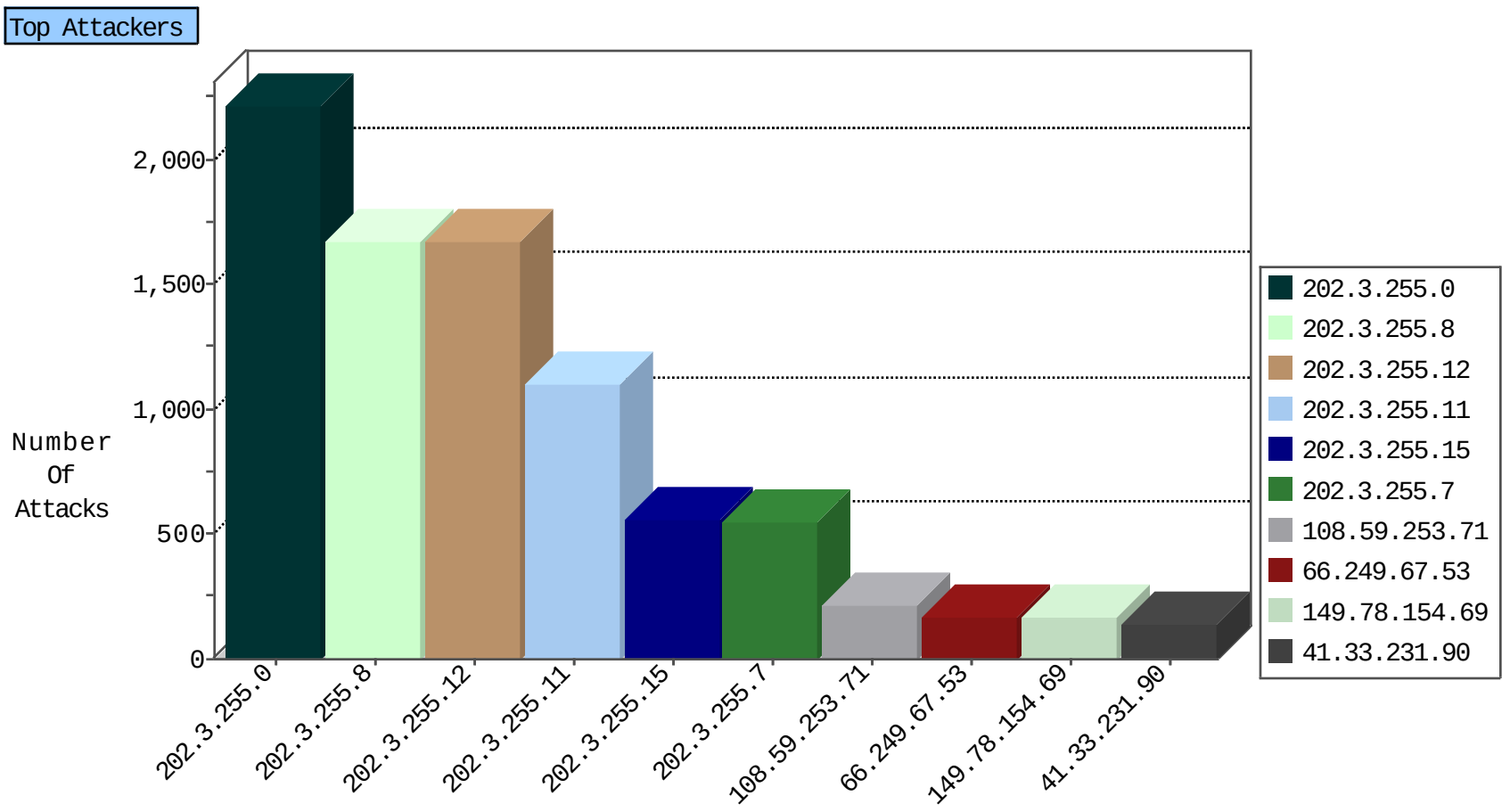
11-10-2015-03:04:02 to 11-10-2015-04:04:02

IDF Under Attack Daily Report





11-10-2015-03:04:02 to 11-10-2015-04:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.74.83	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3967
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2738
66.249.64.181	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	517
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	172
126.22.98.85	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	151
133.46.180.127	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	148
178.44.234.113	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	130
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	106
145.107.166.104	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	83
220.245.31.42	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	81
160.15.11.98	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	76
46.195.152.34	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	73
218.138.174.68	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	68
80.186.40.126	Finland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	58
219.42.50.101	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	57
186.249.237.2	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	57
121.116.66.82	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	55
211.197.4.124	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	53
211.130.66.84	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	51
125.12.248.98	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	50
190.254.92.122	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	47
179.108.176.100	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	46
96.26.237.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	46
171.40.34.74	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	44
150.55.82.48	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	43
66.249.64.17	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	42
122.171.191.104	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41
126.70.75.44	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
120.42.71.25	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
126.127.32.32	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	38
58.105.254.2	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	38
126.23.163.93	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
221.196.136.38	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35
177.30.156.49	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35
119.209.58.52	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32
59.91.172.62	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30
111.254.177.117	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26
126.216.99.8	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26
218.18.80.16	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	16
130.180.216.67	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
24.222.162.87	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
58.238.217.8	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
63.248.161.88	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
8.28.153.102	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
89.29.106.34	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
71.14.172.30	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
89.21.223.2	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
222.186.34.48	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2

11-10-2015-03:04:02 to 11-10-2015-04:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-10-2015-03:04:02 to 11-10-2015-04:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.0	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	2067
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1558
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1557
202.3.255.11	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1030
202.3.255.15	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	524
202.3.255.7	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	514
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
14.215.176.20	147.237.0.15	China	kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.64.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
138.43.71.69	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.28.205.113	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.175.245.100	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.53.74	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
223.4.174.30	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
148.105.174.64	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
14.215.176.21	147.237.0.15	China	kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
193.107.17.72	147.237.76.39	Seychelles	mobile.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.198.180.68	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
136.228.22.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.209.107	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.125.105	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.205.232.40	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.62.1	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.107.17.72	147.237.0.17	Seychelles	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
128.168.219.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
157.231.47.15	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.218.218.1	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.165.58.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.224.110	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.66.50	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
192.101.205.125	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
116.199.134.21	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.145.23.17	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.93.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.118.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.101.186.134	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
134.209.93.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.178.25	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.108.64	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
206.224.181.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.251.106	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.209.58	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
50.204.188.142	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
198.204.3.124	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.221.62	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.82.6	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.117.85	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.106.158.119	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.183.0	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-10-2015-03:04:02 to 11-10-2015-04:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	210
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	152
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	148
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	120
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	119
66.249.67.53	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	118
100.37.165.99	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	112
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	112
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	112
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	100
70.208.72.84	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	91
68.96.59.120	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	90
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	83
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
71.90.130.114	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	67
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
189.217.183.234	Mexico	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
66.249.67.65	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	61
79.178.49.118	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
207.46.13.82	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
66.249.67.53	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
82.205.41.109	Palestinian Territory, Occupied	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
172.56.35.39	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
207.46.13.76	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
162.243.162.27	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
66.249.67.59	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
207.46.13.169	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
151.99.248.178	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
52.28.9.41	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
83.29.154.9	Poland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
79.176.126.15	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
71.191.246.231	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
192.99.12.99	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
207.46.13.107	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
204.93.154.216	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
88.198.157.214	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
105.155.65.82	Morocco	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
40.77.167.9	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	18
66.102.8.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
104.131.94.127	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15

11-10-2015-03:04:02 to 11-10-2015-04:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.215.176.21	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
14.215.176.148	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
14.215.176.149	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
62.90.153.33	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.72.227.17	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/haredim/general.aspx	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8770-he/refuah.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.140	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/×©×§×• ×¤×™×ª×ª 5	Block	1
207.46.13.135	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9736-he/refuah.aspx	Block	1
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
188.40.11.194	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 188.40.11.194	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8910-he/refuah.aspx	Block	1
66.249.64.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
14.215.176.20	China	147.237.0.15	kosher-kravi.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
188.40.11.194	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
41.249.229.10	Morocco	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
72.204.136.105	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8802-he/refuah.aspx	Block	1
14.215.176.20	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.76	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
66.249.69.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/112972.pdf	Block	1

11-10-2015-03:04:02 to 11-10-2015-04:04:02