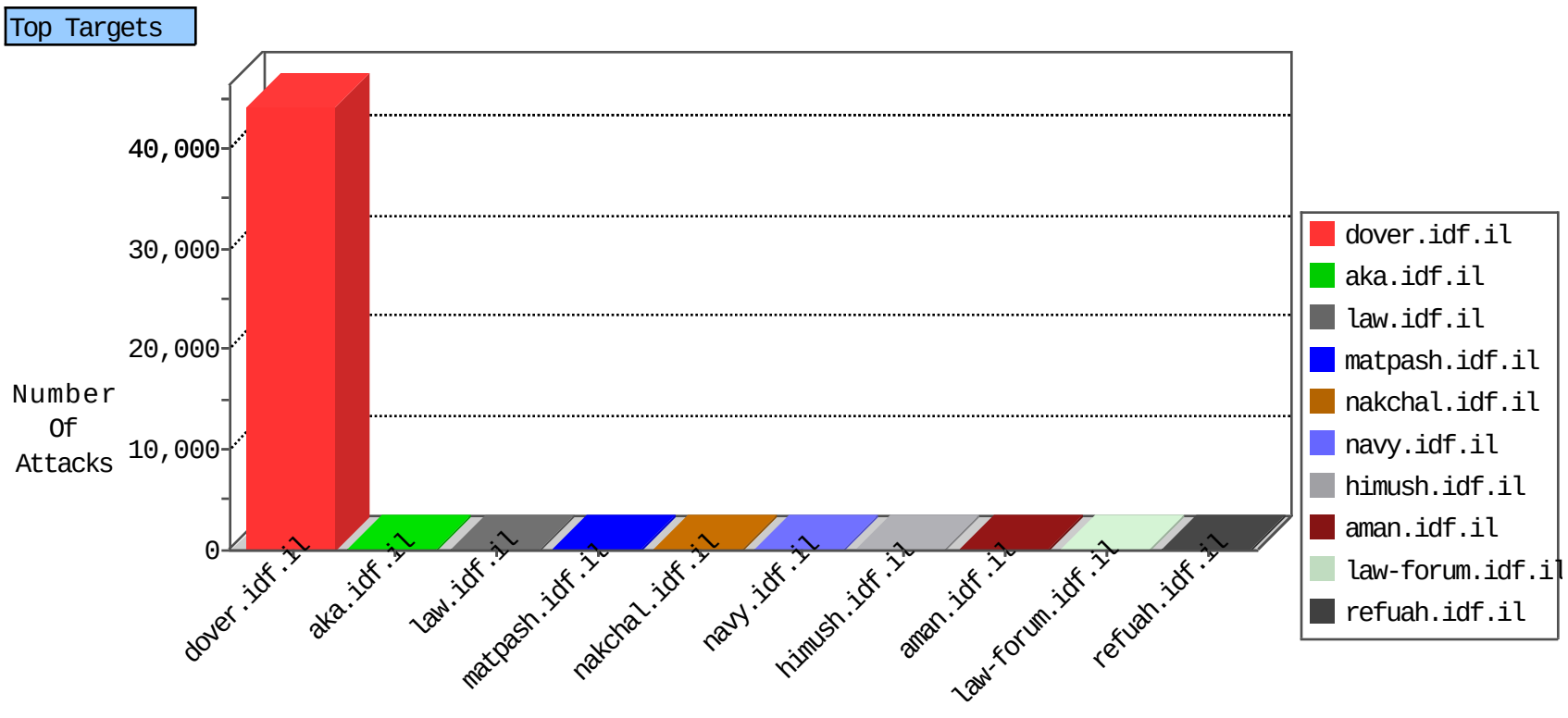
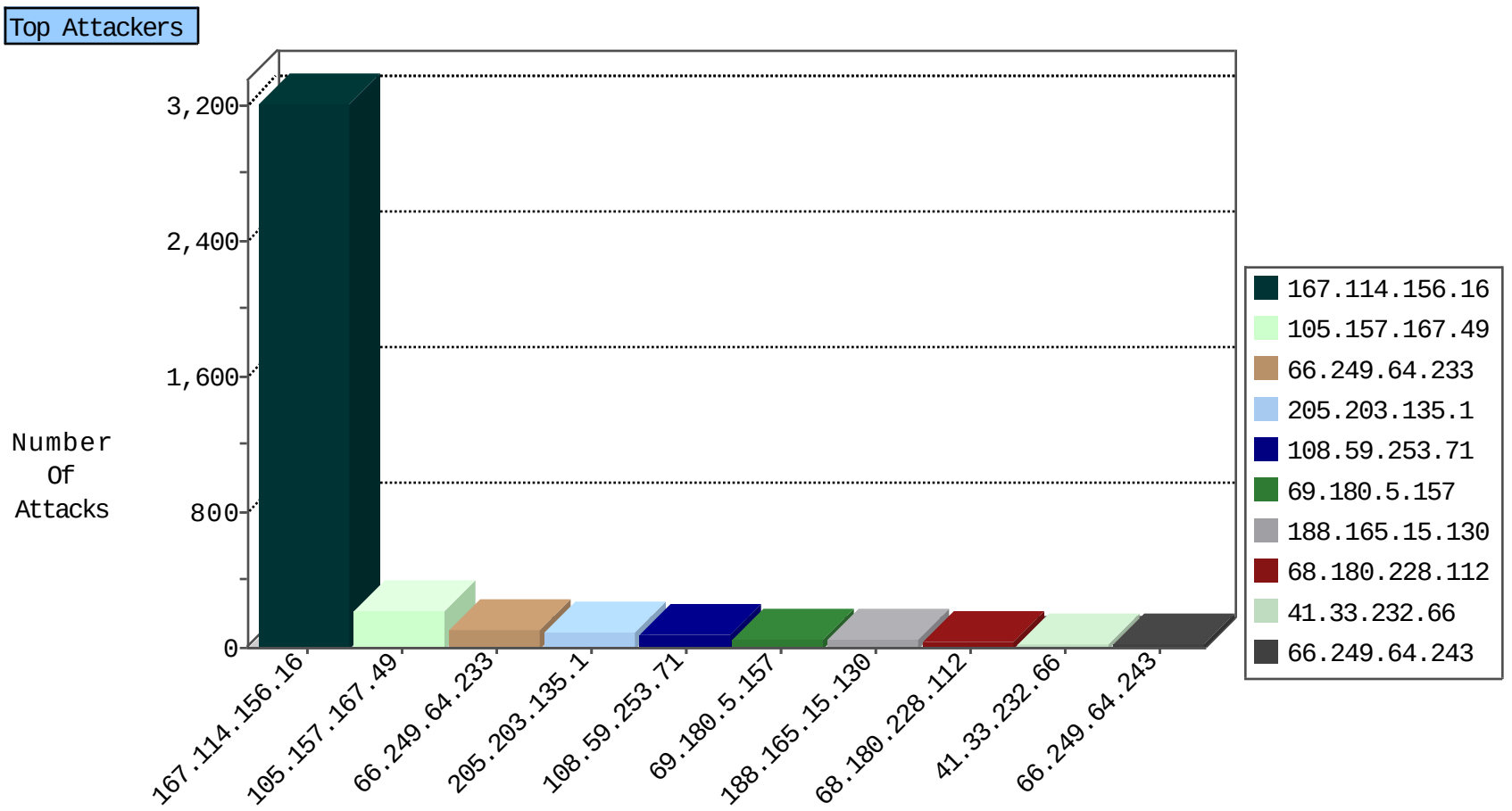
11-15-2015-03:04:02 to 11-15-2015-04:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-15-2015-03:04:02 to 11-15-2015-04:04:02

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	HTTP-POST-Segmented-DoS	dest-reset	744
220.181.108.142	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	207
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	166
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	156
66.249.66.127	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
103.48.136.2		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
24.105.210.108	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
105.235.111.13	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
89.23.232.98	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
74.95.9.8	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
209.98.225.211	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
74.82.245.55	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.139.7	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
2.108.144.46	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
97.66.18.91	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.157.79.69	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.31.253.114	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
204.80.232.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.49.153.71	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
183.104.254.6	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
84.213.18.120	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.162.113.80	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.89.179.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
109.189.97.66	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
77.46.37.71	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.179.91	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.26.10.97	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.94.86.91	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.213.60	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
91.147.235.5	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
68.56.229.87	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.131.88	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.40.56.122	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
174.138.203.122	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
88.132.49.91	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
80.253.191.1	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.197.136.57	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.208.19.27	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
167.88.10.84	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1
209.40.141.66	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
8.24.178.90	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.152.33	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.197.65.13	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.60.82.5	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.175.53.80	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.135.112.91	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.196.165.4	Bulgaria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
50.67.129.3	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
128.111.29.35	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
77.71.15.9	Bulgaria	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-15-2015-03:04:02 to 11-15-2015-04:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.176	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	3
151.80.31.147	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	3
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	3
188.165.15.202	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.36	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.131	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
198.245.51.90	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

11-15-2015-03:04:02 to 11-15-2015-04:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
119.38.224.98	147.237.77.216	China	dover.idf.il	GPL SCAN nmap TCP	4
203.86.7.130	147.237.77.216	China	dover.idf.il	GPL SCAN nmap TCP	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
136.228.221.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.236.26	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.131.104.12	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
189.115.111.243	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
200.105.46.6	147.237.77.216	Argentina	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.204.124	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
41.140.253.9	147.237.77.243	Morocco	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
167.28.136.10	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.72.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.205.227.9	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
150.126.38.38	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.130.154.68	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
180.120.242.212	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
136.228.147.44	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.135.131.20	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
40.115.58.160	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
167.28.35.30	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
129.76.107.45	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.198.184.86	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.198.179.96	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.227.103	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.48.195	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.99.6	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.223.48	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.6.71.154	147.237.8.24	Poland	e.lifestyle.idf.	ET SCAN NMAP -sS window 1024	1
162.125.177.56	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.207.126	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.34.184.74	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
143.49.182.108	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.248.200.109	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.238.181.56	147.237.77.216	Germany	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.247.24	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.209.141.68	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.148.79.105	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.110.76	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.168.207.78	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.205.79.80	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.208.55	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
1.235.195.234	147.237.77.19	Korea, Republic of	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
85.17.239.155	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
170.120.123.71	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.172.139.108	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.98.225.211	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
148.248.76.56	147.237.77.216	Mexico	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
162.125.88.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
121.46.105.50	147.237.77.216	China	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
198.162.208.25	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-15-2015-03:04:02 to 11-15-2015-04:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3093
105.157.167.49	Morocco	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	213
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	90
66.249.64.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	86
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	79
69.180.5.157	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
188.165.15.130	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	43
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
149.78.154.69	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
66.249.64.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
104.131.195.214	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
188.165.15.233	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	11
46.19.86.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
66.249.64.243	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
79.183.183.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
79.183.183.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
157.55.39.135	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
5.28.143.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
5.28.143.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
67.87.221.105	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	6
54.186.248.49	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
65.19.138.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
66.102.8.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
66.249.64.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
70.198.193.67	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
109.66.199.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.141.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
40.77.167.45	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
93.172.139.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
93.172.139.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.67.105.87	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
173.33.196.119	Canada	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
207.46.13.91	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
207.46.13.95	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
17.142.156.109	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4

11-15-2015-03:04:02 to 11-15-2015-04:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	7
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
173.33.196.119	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	2
5.28.143.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.115.111.73	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
40.77.167.45	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
109.67.27.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.95	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.66.95	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.102.8.243	Block	1
113.11.250.211	Singapore	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.66.127	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/229-he/faq.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
207.46.13.60	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/	Block	1
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1

11-15-2015-03:04:02 to 11-15-2015-04:04:02