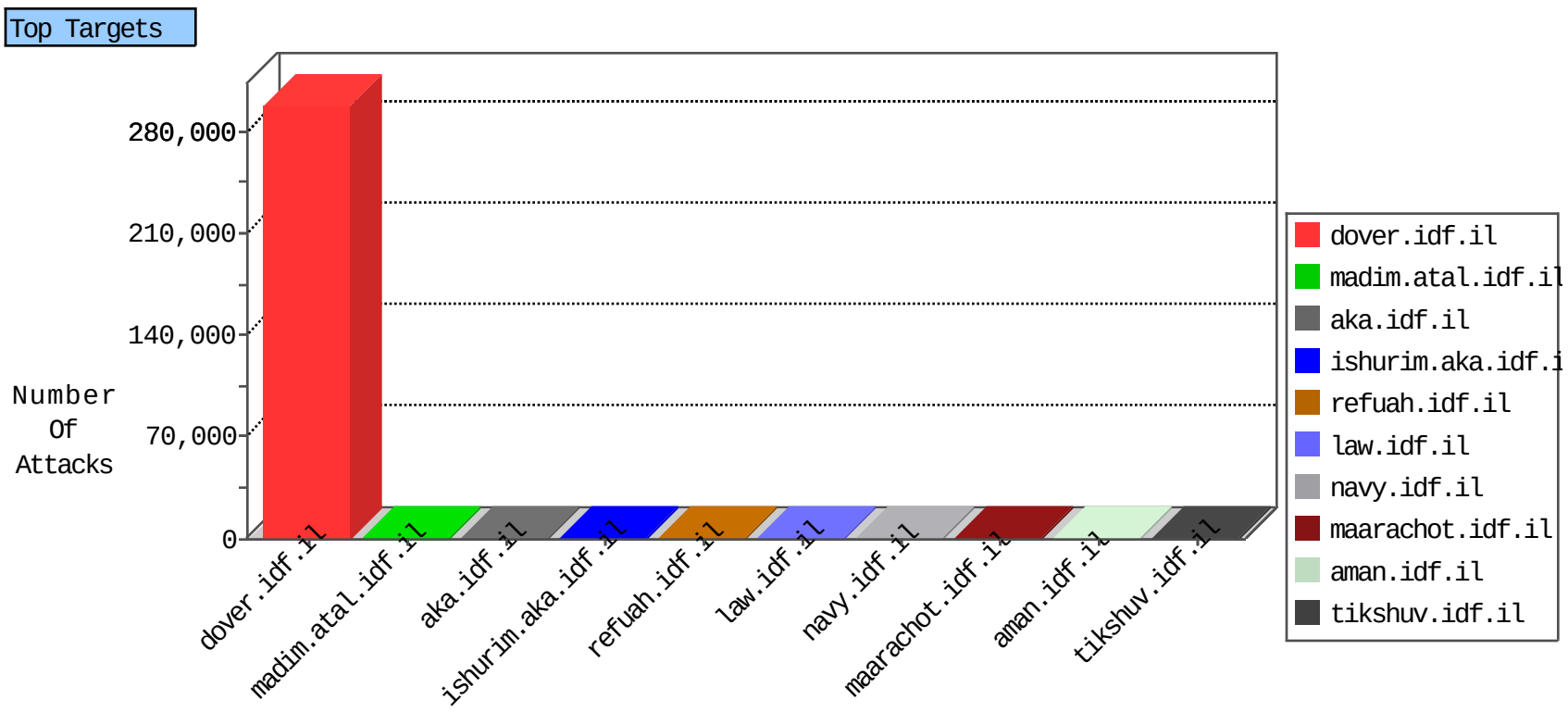
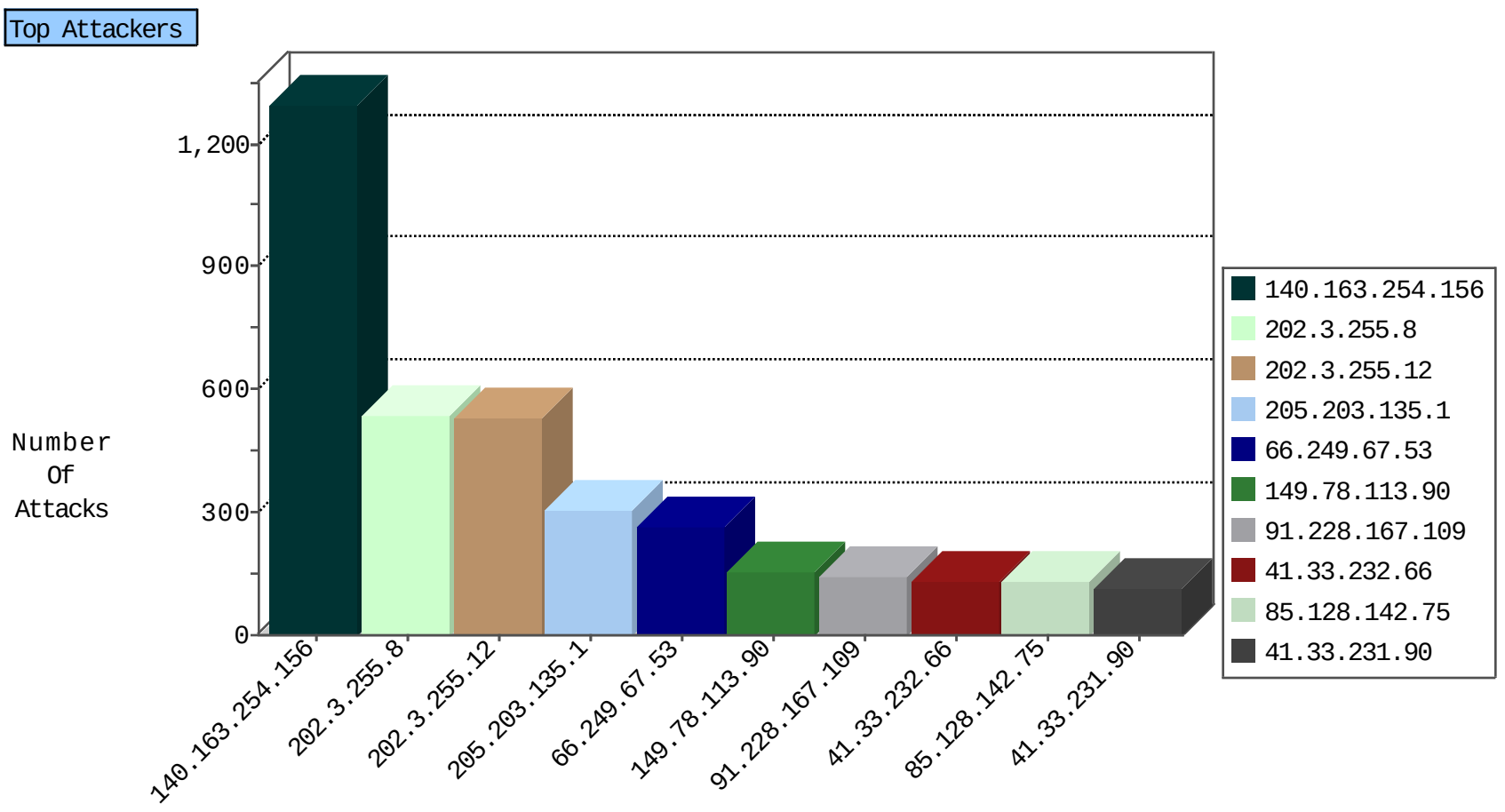
11-19-2015-01:06:52 to 11-19-2015-02:06:52

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-19-2015-01:06:52 to 11-19-2015-02:06:52

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11082
119.196.131.12	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5861
96.57.168.114	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5455
186.29.79.18	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3199
175.116.32.123	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2908
31.186.228.30	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2847
159.203.246.114	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2831
113.170.247.77	Vietnam	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2824
36.234.126.21	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2728
116.138.1.91	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2677
220.91.79.31	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	593
142.4.127.67	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	235
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	173
222.110.170.69	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	123
179.178.129.106	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	103
221.239.247.101	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	59
112.162.134.74	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41
163.18.77.7	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35
46.19.85.125	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	13
109.65.205.242	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
93.173.43.159	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
176.13.2.205	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
173.34.75.63	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
187.87.254.65	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
60.249.199.71	Taiwan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
94.255.180.106	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
188.113.97.52	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
176.13.15.91	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
155.4.97.89	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
185.32.179.96	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
198.48.190.72	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
94.135.219.80	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
209.40.162.68	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
210.105.106.97	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
72.2.17.96	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
112.231.43.127	China	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
207.213.182.102	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
37.148.225.58	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.236.36.45	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.48.25.1	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
86.48.76.69	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.60.241.41	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
104.230.143.55		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
200.84.203.71	Venezuela	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
31.209.35.98	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-19-2015-01:06:52 to 11-19-2015-02:06:52

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-19-2015-01:06:52 to 11-19-2015-02:06:52

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	498
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	494
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	2
82.192.68.46	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.67.53	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
136.228.77.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
167.97.4.29	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.172.140	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
192.240.155.234	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
206.15.106.34	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
148.105.169.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.44.134.80	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.176.60	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
113.108.21.16	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
167.28.43.70	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.32.179.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
134.209.117.58	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.105.74.115	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
63.141.45.30	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.113.98.116	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
113.108.21.16	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
206.15.106.34	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
159.223.221.33	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.178.207.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
181.196.89.89	147.237.8.28	Ecuador	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
134.172.158.13	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.54.39.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.38.250.31	147.237.77.74	Greece	law.idf.il	ET SCAN NMAP -sS window 3072	1
170.106.184.24	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
110.232.164.122	147.237.77.216	Philippines	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.106.214.17	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
147.50.146.124	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.94.2	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.110.183.50	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.47.232.0	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
134.127.136.72	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.170.88	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.217.253.99	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.249.90	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
74.117.209.135	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.47.87.11	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.201.87.10	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
217.147.86.118	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
157.231.57.22	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.85.37	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.216.171.90	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
201.7.216.54	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-19-2015-01:06:52 to 11-19-2015-02:06:52

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
140.163.254.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1292
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	174
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	143
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
85.128.142.75	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
66.249.67.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
37.142.178.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
37.26.146.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
2.54.157.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
212.199.57.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
166.216.157.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
52.33.219.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
52.0.238.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.227.118.21	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
207.46.13.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
109.64.163.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
79.182.219.246	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
85.65.34.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
89.138.175.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.13.23.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.13.2.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
79.181.34.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.67.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
75.74.10.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
37.26.149.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.87.3.242	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
88.198.157.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
72.234.181.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
203.135.187.11	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
204.93.154.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19

11-19-2015-01:06:52 to 11-19-2015-02:06:52

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.113.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
149.78.113.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.88.244.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
2.52.150.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.109.113.161	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.116.223.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
141.212.122.96	United States	147.237.0.15	kosher-kravi.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.67.53	Block	1
84.42.132.75	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
46.117.81.248	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method .aspx?&l=he&f=1133&d=22943 in URL	Block	1
141.212.122.96	United States	147.237.76.200	eitan.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
2.54.12.148	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3468.gif	Block	1
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.5.211	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/ufi/reaction/	Block	1
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
207.46.13.128	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.236.37.210		147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-he/tikshuv.aspxshared/usercontrols/headerupper/	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3156.jpg	Block	1
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
207.46.13.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
131.162.130.180	Canada	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

11-19-2015-01:06:52 to 11-19-2015-02:06:52