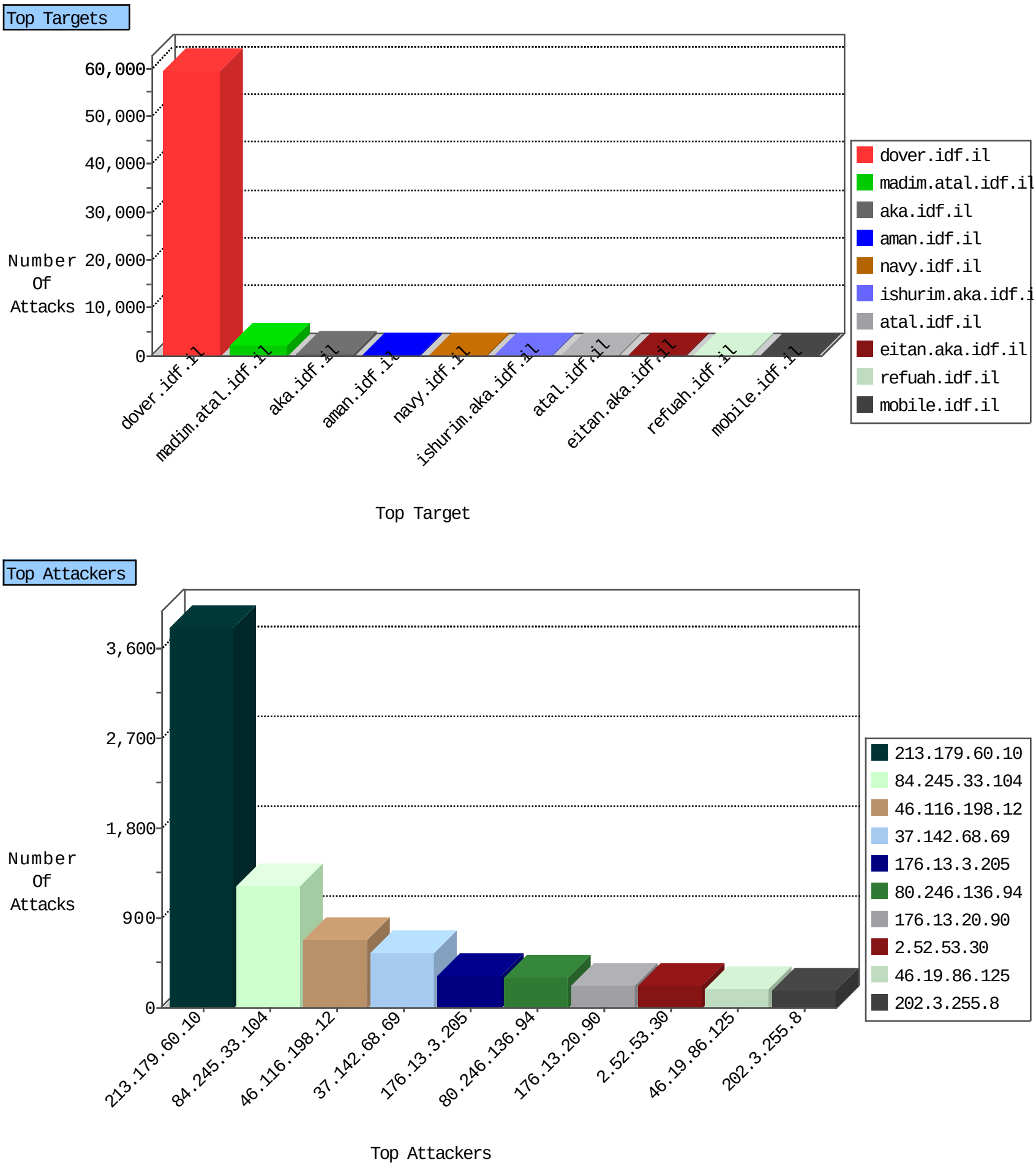
11-20-2015-11:04:06 to 11-20-2015-12:04:06

IDF Under Attack
Daily Report



11-20-2015-11:04:06 to 11-20-2015-12:04:06

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	DOS-Tool-SwitchbladG	dest-reset	48
79.182.150.177	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
89.233.198.2	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
12.108.54.77	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
162.246.10.10	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
94.135.206.99	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.234.248.88	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
139.91.68.4	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.240.192.138	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
189.79.165.35	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.29.93	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
141.212.121.204	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
68.235.179.26	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-20-2015-11:04:06 to 11-20-2015-12:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.179.60.10	United Kingdom	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1000
84.245.33.104	Netherlands	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	721
84.245.33.104	Netherlands	147.237.77.216	dover.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	377
74.208.133.60	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
213.179.60.10	United Kingdom	147.237.77.216	dover.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	7
84.245.33.104	Netherlands	147.237.77.216	dover.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	4
23.99.3.91	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
23.99.3.101	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
23.99.3.100	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
192.96.206.187	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

11-20-2015-11:04:06 to 11-20-2015-12:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.179.60.10	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	2366
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	134
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	132
74.208.133.60	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	10
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
136.228.86.43	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
201.71.6.16	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.212.45.112	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.12.151.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
170.113.206.54	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
54.176.4.242	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
170.67.177.63	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.117.128.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.28.113.41	147.237.77.216	Chile	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.210.189.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
150.126.1.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.205.221.21	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
148.178.15.84	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
204.147.253.34	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
138.43.67.54	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.86.76.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.47.7.124	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.200.176.74	147.237.77.216		dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.120.2.23	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
64.112.91.24	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
170.106.91.109	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
50.18.225.195	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
167.97.227.11	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
159.223.134.13	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.151.50.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.8.45	Poland	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
148.178.82.120	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.182.64.114	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.170.180.112	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

11-20-2015-11:04:06 to 11-20-2015-12:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.179.60.10	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	441
46.19.86.125	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	186
176.13.9.44	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
84.245.33.104	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
194.39.218.10	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.26.148.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
176.13.20.90	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
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
46.19.86.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
192.117.148.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.66.252.209	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
178.25.3.243	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
189.202.55.91	Mexico	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
41.185.31.40	South Africa	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	24
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.146.39.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
5.22.129.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.52.145.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
159.122.86.190	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.54.132.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
176.13.20.90	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
2.52.156.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
87.203.103.152	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
2.54.132.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.178.97.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
82.205.73.239	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.178.97.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
80.178.138.115	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
80.178.138.115	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.87.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
109.65.81.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.204	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.64.76.147	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
85.250.124.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
95.150.62.145	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

11-20-2015-11:04:06 to 11-20-2015-12:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.198.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	429
37.142.68.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	286
176.13.3.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	195
80.246.136.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	143
37.142.68.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	135
46.116.198.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	128
46.116.198.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
176.13.20.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
37.142.68.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
176.13.3.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
2.52.53.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
80.246.136.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.52.53.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	82
80.246.136.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	53
176.13.20.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
2.52.7.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
2.52.53.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	29
176.13.3.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	13
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.116.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.253.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/61193.pdf.	Block	3
84.111.66.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.141.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.3.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.168.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.178.15.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
192.117.148.166	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
176.13.6.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.90.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.13.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.3.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
84.228.74.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.136.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.211.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
84.108.47.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
213.151.39.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/&sa=u&ved=0ahukewimo8dr2z7jahukohqkhc7rddiqfgghmaa&usg=afqjcnh4ucr3bqpmkvh4yz9t7jscutsloq	Block	1
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method c=%5B%22%22%2C%22%22%2C1448011936%2C%22http%3A%2F%2Fm.facebook.com%2F%22%5D; in URL _pk_id.20.8afc=fc48031c091395bc.1416567320.11.1448011936.1448011936.	Block	1
74.82.47.3	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/17281.jpg	Block	1
37.26.149.171	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

11-20-2015-11:04:06 to 11-20-2015-12:04:06