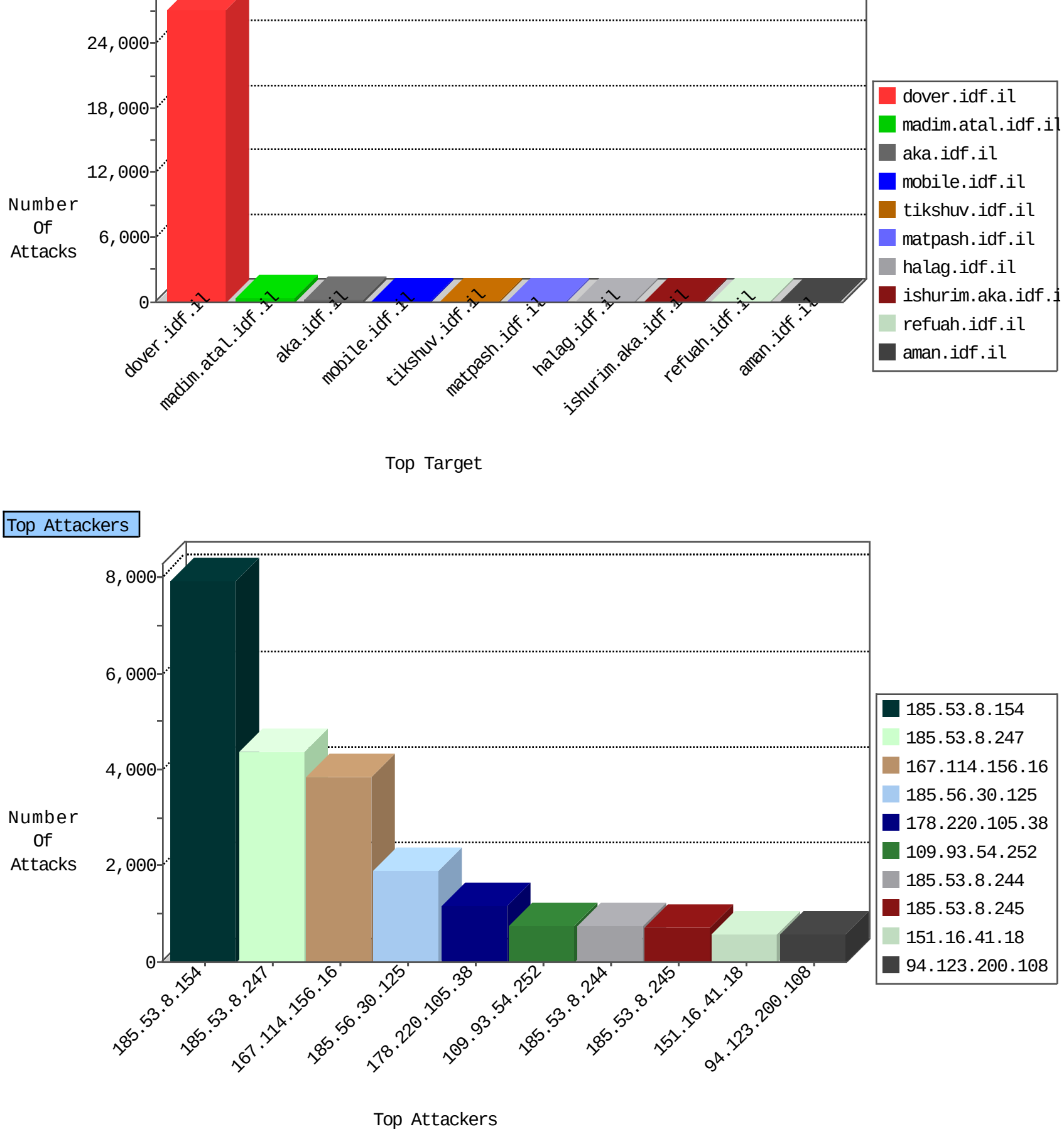
04-11-2016-17:04:01 to 04-11-2016-18:04:01

IDF Under Attack Daily Report



04-11-2016-17:04:01 to 04-11-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	14009
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	13010
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3837
179.252.43.27	Brazil	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	157
179.252.43.27	Brazil	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	138
197.2.106.182	Tunisia	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	91
197.2.106.182	Tunisia	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	73
132.3.53.78	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	66
132.3.53.80	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	62
93.63.226.141	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	58
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
84.110.108.153	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
87.69.231.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
80.178.157.42	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	3
202.140.108.137	Hong Kong	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	3
158.169.40.9	Belgium	147.237.77.176	matpash.idf.il	JLM_Purple_Con_Limit_Http	drop	3
66.249.93.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
125.65.46.143	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
202.166.81.250	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
158.169.40.9	Belgium	147.237.77.176	matpash.idf.il	JLM_Under_Attack_Con_Http	drop	2
80.82.78.38	Netherlands	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
202.140.108.92	Hong Kong	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
179.43.141.194	Switzerland	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
62.138.2.122	Germany	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
79.179.133.17	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
202.140.108.93	Hong Kong	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
82.145.221.177	Europe	147.237.72.14	dover.idf.il(old)	Block_Ip_Web_In	drop	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
202.140.108.83	Hong Kong	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
108.59.8.70	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
202.140.108.94	Hong Kong	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
202.140.108.89	Hong Kong	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
179.43.141.194	Switzerland	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
109.64.145.241	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-11-2016-17:04:01 to 04-11-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.143.110.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
37.26.148.237	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
213.57.188.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
94.123.200.108	Turkey	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	3
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.147.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
185.106.92.47	Russian Federation	147.237.72.156	aman.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
144.76.7.107	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
85.64.49.108	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.85	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.190	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-11-2016-17:04:01 to 04-11-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.123.200.108	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	8
94.123.200.108	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP login.htm access	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
84.95.252.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.8.50	Latvia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.164.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
112.112.56.65	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.67.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.123.200.108	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP adminlogin access	1
84.109.209.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.169.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.115.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.8.28	Latvia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.107.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
164.138.23.232	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.31.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.112.56.157	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.145.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-11-2016-17:04:01 to 04-11-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.53.8.154	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7947
185.53.8.247	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4371
185.56.30.125	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1916
178.220.105.38		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1179
109.93.54.252		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	747
185.53.8.244	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	738
185.53.8.245	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	716
151.16.41.18	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	581
121.54.44.89	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	537
177.23.207.221	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	464
79.215.228.169	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	402
87.151.231.53	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	335
148.0.182.157	Dominican Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
121.54.44.93	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	227
202.140.108.86	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
202.140.108.99	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
202.140.108.116	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
202.140.108.119	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
202.140.108.111	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
202.140.108.88	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
197.2.106.182	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	51
158.169.40.9	Belgium	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	50
202.140.110.55	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
202.140.110.54	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
202.140.108.126	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
202.140.108.92	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
202.140.108.94	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
202.140.108.137	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
202.140.108.89	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
202.140.108.85	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
202.140.108.127	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
202.140.108.91	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
202.140.108.90	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.140.108.95	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.140.108.115	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
202.140.108.87	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
109.253.216.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
80.246.133.31	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
202.140.108.96	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
202.140.108.100	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
202.140.108.136	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
202.140.108.84	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
84.134.172.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
202.140.108.93	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
132.3.53.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
99.164.5.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
132.3.53.80	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
121.54.44.90	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.26.146.189	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18

04-11-2016-17:04:01 to 04-11-2016-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.123.200.108	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.123.200.108	Block	219
94.123.200.108	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 94.123.200.108	Block	205
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	179
94.123.200.108	Turkey	147.237.77.216	dover.idf.il	PHP Attempt	Block	121
95.35.24.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
95.35.206.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
217.132.119.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
109.253.206.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
109.253.216.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
185.32.179.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.55.55.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
157.55.2.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.93.119	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
63.139.48.66	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.193	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx	Block	2
79.177.9.133	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
65.55.210.254	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.16.48	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	2
213.87.103.133	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	2
185.32.179.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.197.232	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.1.179	Israel	147.237.77.243	mobile.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
199.30.24.64	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.93.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.87.103.133	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	2
85.96.51.149	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
188.120.148.138	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
46.19.85.5	Israel	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Illegal Byte Code Character in Method 3yT,=ÅT™ä©Ã[[#2]]Ì†«Ó)gýW”nI ¤ÄKžJ£*hò¨Xf•Œ ¾‰~-‘`5@[[#24]]–[[#1]]€šB	Block	1
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
199.30.25.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.133.31	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
66.249.93.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.182.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.2.132	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
108.227.98.31	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.116.220.81	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	1
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
188.120.148.138	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15133-he/	Block	1
87.69.224.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
46.19.85.5	Israel	147.237.77.74	law.idf.il	Malformed URL	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Unknown HTTP Request Method 3yT,=ÅT™ä©Ã[[#2]]Ì†«Ó)gýW”nI ¤ÄKžJ£*hò¨Xf•Œ ¾‰~-‘`5@[[#24]]–[[#1]]€šB in URL	Block	1
79.178.147.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19926-he/dover.aspx	Block	1
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
212.199.143.110	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	1

04-11-2016-17:04:01 to 04-11-2016-18:04:01