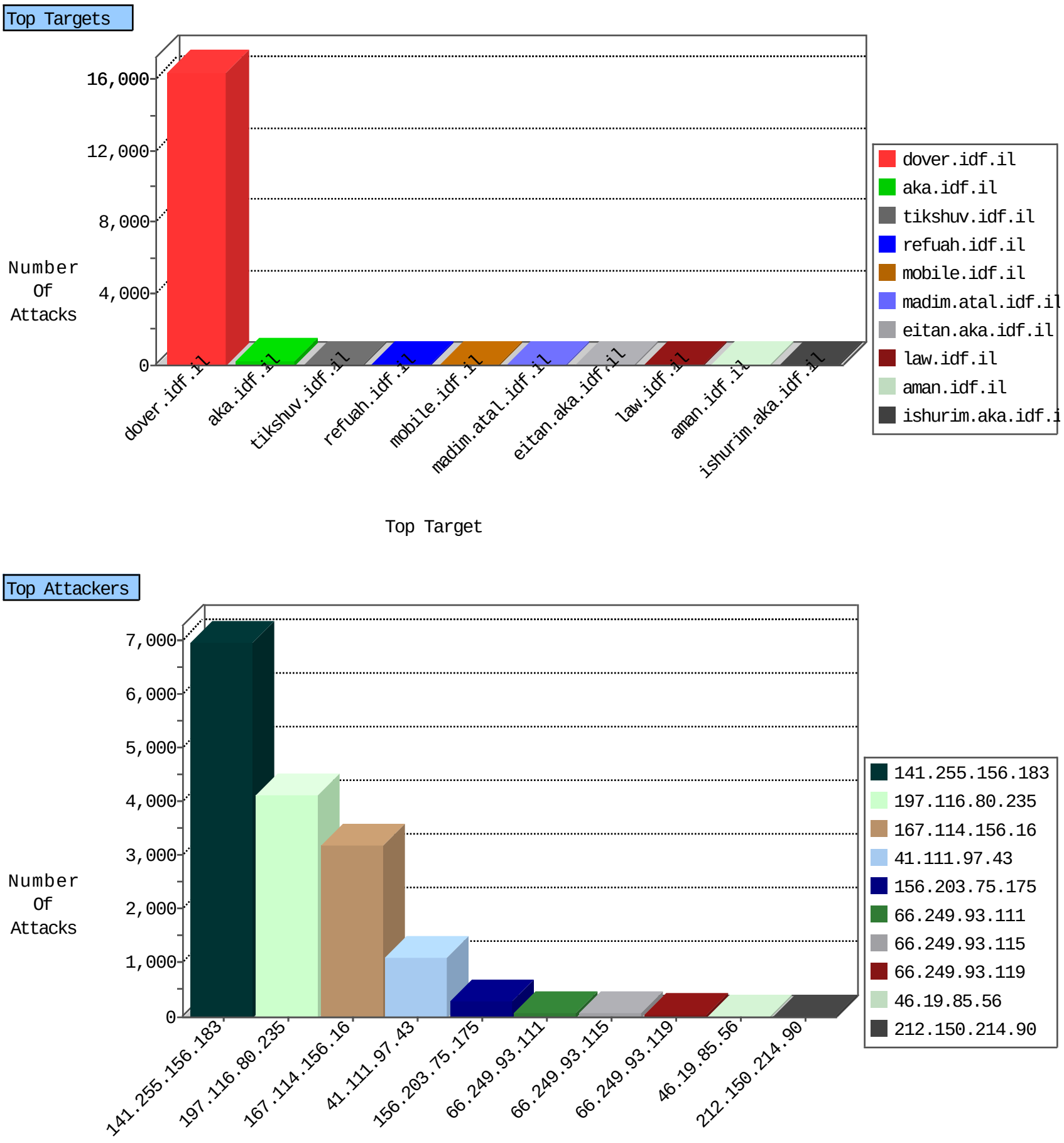
04-11-2016-23:04:09 to 04-12-2016-00:04:09

IDF Under Attack
Daily Report



04-11-2016-23:04:09 to 04-12-2016-00:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	7642
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3186
41.111.97.43	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1087
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	645
31.210.187.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	641
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	641
109.253.224.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	625
94.159.151.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	506
5.28.191.233	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	473
79.168.49.63	Portugal	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	406
83.130.116.167	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	355
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	250
80.178.157.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	183
156.203.75.175	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	142
87.70.88.156	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	136
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	98
105.158.169.76	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	96
41.111.97.43	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	65
167.102.190.106	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	58
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	17
84.240.57.96	Lithuania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	7
46.19.85.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-lgn	dest-reset	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
46.19.85.88	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
109.66.14.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
79.178.224.35	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.86.11	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
149.78.248.39	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
207.107.118.46	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.97.106.161	China	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
5.102.254.17	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
96.229.186.202	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
92.222.65.232	France	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
79.179.54.35	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.139	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.97.106.162	China	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
72.218.35.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
92.222.65.232	France	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
79.180.206.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.249	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.97.106.162	China	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
149.78.47.140	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
41.109.168.136	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.65.252.110	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
213.8.204.63	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-11-2016-23:04:09 to 04-12-2016-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.111.97.43	Algeria	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	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
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.93.101	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.93.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-11-2016-23:04:09 to 04-12-2016-00:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
208.80.155.215	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3
212.106.92.100	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
186.114.35.239	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.184.2.29	147.237.77.233	Japan	atal.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
220.231.195.122	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN NMAP -sS window 3072	1
208.100.26.228	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
122.155.162.71	147.237.77.74	Thailand	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.131	147.237.76.202	Canada	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
42.243.84.74	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN NMAP -sS window 4096	1
13.92.81.18	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
213.151.32.163	147.237.76.31	Israel	nakchal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
208.100.26.228	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

04-11-2016-23:04:09 to 04-12-2016-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6903
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1403
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	170
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
156.203.75.175	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	62
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
156.203.75.175	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
156.203.75.175	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
212.106.92.100	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	SYN Attack		reject	15
185.3.144.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
95.86.122.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.176.104.8	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.149.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
156.203.75.175	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN was acknowledged. Stripping all packet data.	drop	7
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
164.138.116.200	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.121.99.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.54.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.133	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.2.205	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.210.187.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.219.230.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.46.45.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.240.57.96	Lithuania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.128	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.167.102	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 93.173.167.102	Block	11
2.52.168.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.254	Block	4
65.55.210.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.9.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
89.138.211.222	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 89.138.211.222	None	3
199.30.24.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.162	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.196.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.229	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.16.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.181.57.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.111.137.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	2
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
5.29.189.149	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.241	Block	1
85.65.116.235	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 103 cookies	Block	1
146.115.145.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
37.144.77.55	Russian Federation	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
93.173.167.102	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
207.46.13.62	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.aspx)	Block	1
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.241	Block	1
114.97.195.129	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1819-he/idfg.aspx/trackback/	Block	1
89.138.211.222	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
149.88.3.7	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
37.144.77.55	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
95.86.104.83	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
213.57.33.131	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method h55 in URL	Block	1
176.13.14.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
130.203.139.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/	Block	1
149.88.197.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.160.168.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
82.102.234.225	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
46.116.52.172	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
180.76.15.13	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	Block	1
137.132.250.8	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.83.88.34	Hungary	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
156.203.75.175	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
109.160.168.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1