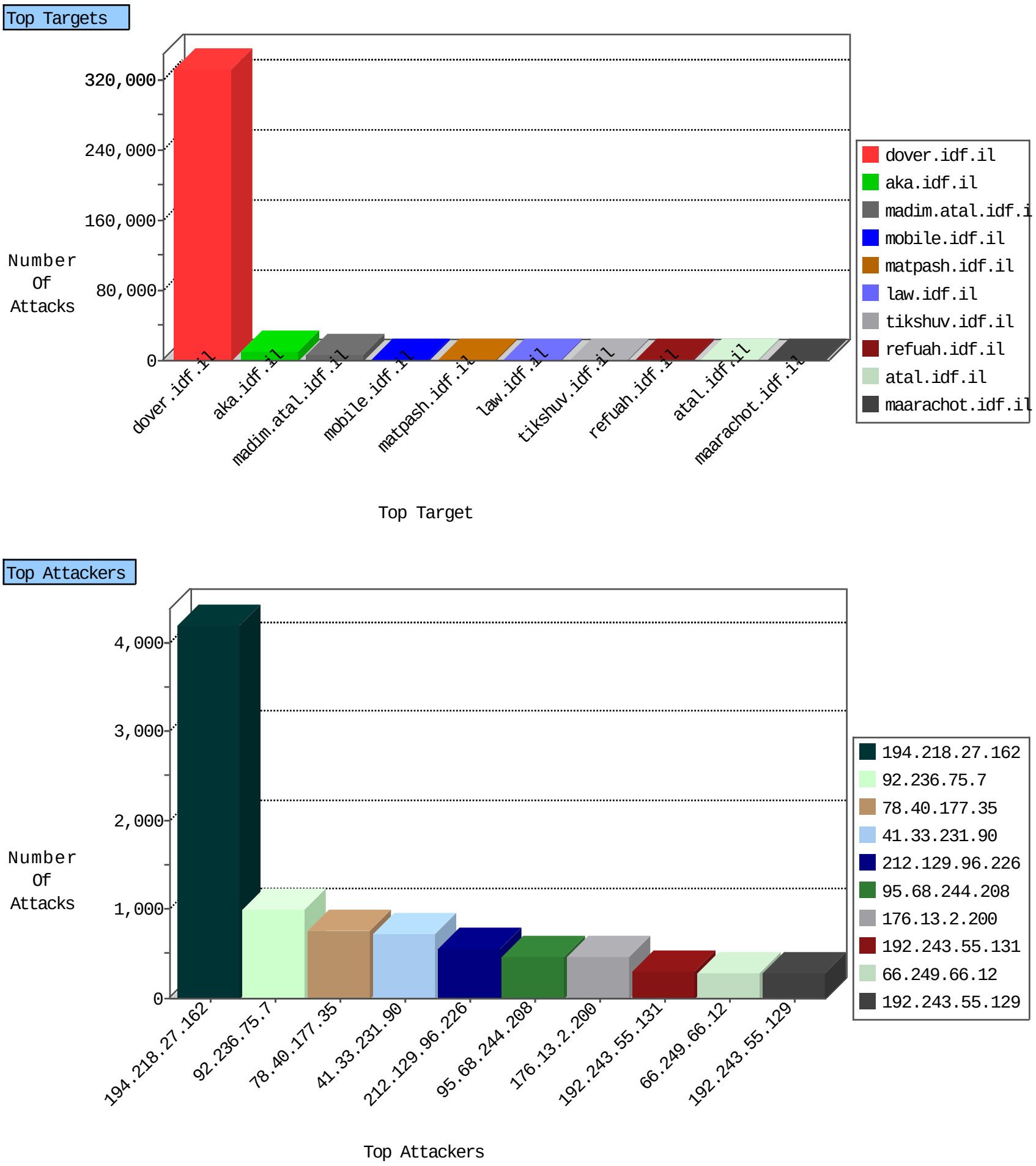
03-02-2016 to 03-03-2016

IDF Under Attack
Daily Report



03-02-2016 to 03-03-2016

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	network flood IPv4 UDP	drop	2998155
48.134.97.193	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37713
75.74.68.25	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37186
93.225.119.227	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36773
114.201.207.165	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36727
62.196.20.133	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36645
254.75.87.241		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36640
64.210.7.110	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36535
225.70.227.37		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36519
214.6.160.161	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36392
201.153.26.107	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36390
198.58.250.46	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36382
48.83.204.66	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36363
48.131.196.189	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36356
71.132.121.215	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36309
144.128.156.111	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36301
193.137.6.155	Portugal	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36230
19.135.190.189	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36164
231.203.236.255		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36140
232.158.119.149		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36084
113.145.103.223	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36055
18.175.203.248	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35894
49.69.212.179	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35844
95.217.236.86	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35835
62.26.93.122	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35815
99.246.148.127	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35810
216.206.154.150	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35798
193.163.255.217	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35756
160.208.183.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35672
1.58.211.200	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35663
101.195.118.204	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35661
160.20.38.113	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35642
95.244.137.168	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35551
73.151.81.143	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35546
36.18.120.202	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35527
223.67.27.185	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35477
63.101.22.174	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35474
250.108.101.207		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35432
149.252.208.255	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35417
50.63.11.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35402
191.48.136.46	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35389
64.36.113.152	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35369
228.245.255.101		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35310
246.232.178.10		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35282
219.102.86.8	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35282
143.102.202.244	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35248
117.193.119.169	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35188
76.180.143.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35136
0.140.216.74		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35070
105.115.172.150	Nigeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35041

03-02-2016 to 03-03-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
87.68.249.53	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	21
106.38.241.107	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
61.135.189.119	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	18
79.182.50.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
87.71.90.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
109.64.73.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
157.55.39.210	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
79.179.128.52	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
81.218.101.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
37.46.41.242	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
46.19.86.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
81.218.251.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
5.102.206.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.108.9.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.108.227.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
147.235.185.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
31.154.94.62	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
77.126.66.233	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.183.99.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
89.139.158.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.110.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.78.96.54	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
176.13.14.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
176.228.30.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.85.216	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
84.109.113.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
147.236.31.231	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
37.142.68.11	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.230	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.117.250.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.183.16.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
95.86.65.164	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.66.134.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
149.78.150.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
185.24.207.49	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.8.10.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
93.173.44.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
172.19.203.101		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
213.57.209.45	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
2.54.9.81	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.176.80.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4

03-02-2016 to 03-03-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	286
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	40
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	16
92.236.75.7	147.237.77.216	United Kingdom	dover.idf.il	WEB-MISC Chunked-Encoding transfer attempt	11
158.69.206.202	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	10
52.48.63.203	147.237.72.166	United States	aka.idf.il	Tehila - Perl LWP with fake user agent	6
80.246.130.37	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
176.13.22.37	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	4
80.246.133.222	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
46.151.52.139	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
149.88.85.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.133.89	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
109.66.155.232	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
92.236.75.7	147.237.77.216	United Kingdom	dover.idf.il	SERVER-WEBAPP TRACE attempt	2
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
37.26.148.221	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
46.151.52.139	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	2
85.64.2.84	147.237.76.30	Israel	himush.idf.il	ET SCAN NMAP -sA (2)	2
89.139.247.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
213.151.47.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
92.236.75.7	147.237.77.216	United Kingdom	dover.idf.il	SERVER-WEBAPP DELETE attempt	2
199.203.62.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.48.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.221	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
113.76.90.199	147.237.77.243	China	mobile.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
45.32.49.30	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
95.217.174.35	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
210.117.121.60	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.7.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.109.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.254.90.133	147.237.77.205	Mexico	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
79.176.158.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.122.254.212	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
27.201.220.123	147.237.77.121	China	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.114	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.160.254.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.211.77.35	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.26.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.165.135.130	147.237.77.121	Germany	e.navy.idf.il	ET SCAN Potential SSH Scan	1
187.58.224.213	147.237.72.166	Brazil	aka.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.64.190	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	1
137.226.113.7	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1

03-02-2016 to 03-03-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2803
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1399
92.236.75.7	United Kingdom	147.237.77.216	dover.idf.il	Command Injection	command injection detected in request: 'Sh'	monitor	754
78.40.177.35	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	718
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	686
176.13.2.200	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	160
100.15.90.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
185.118.27.11		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	135
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	125
185.118.27.8		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
185.118.27.9		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
185.118.27.14		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
185.118.27.10		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
185.118.27.13		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
185.118.27.7		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
194.90.151.18	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	93
185.118.27.15		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
185.118.27.12		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
176.13.2.200	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	80
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	77
176.13.19.56	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	66
82.166.42.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	65
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	61
2.52.38.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
41.206.148.11	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
5.102.227.92	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
92.236.75.7	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
93.42.131.120	Italy	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
109.253.215.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
176.13.18.43	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
107.167.112.31	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	46
108.53.49.9	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
79.183.26.175	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
109.66.195.234	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
89.206.52.99	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
2.54.38.25	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
109.67.123.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
173.208.130.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
185.32.179.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
192.115.177.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
31.154.148.177	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
95.159.5.92	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
176.13.19.56	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	33
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	32

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.11.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	277
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	233
176.13.7.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	224
46.19.85.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	222
176.13.2.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	214
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	209
82.80.131.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	200
109.253.144.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	200
46.19.85.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	185
2.54.140.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	174
176.13.19.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
176.13.11.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
2.54.36.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
176.13.16.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
46.19.86.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
37.26.148.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
80.246.136.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
79.181.54.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
2.52.0.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
46.19.85.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
176.13.15.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
2.52.158.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
5.28.177.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
109.253.147.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
185.32.179.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
46.19.85.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
109.253.220.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
2.52.143.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
109.253.202.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.54.3.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
2.52.2.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
80.246.136.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
176.13.22.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
176.13.13.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
2.54.150.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
2.54.140.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
80.246.136.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
176.13.6.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
109.253.215.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
2.52.132.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.13.15.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.54.36.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	34
109.65.113.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34

03-02-2016 to 03-03-2016