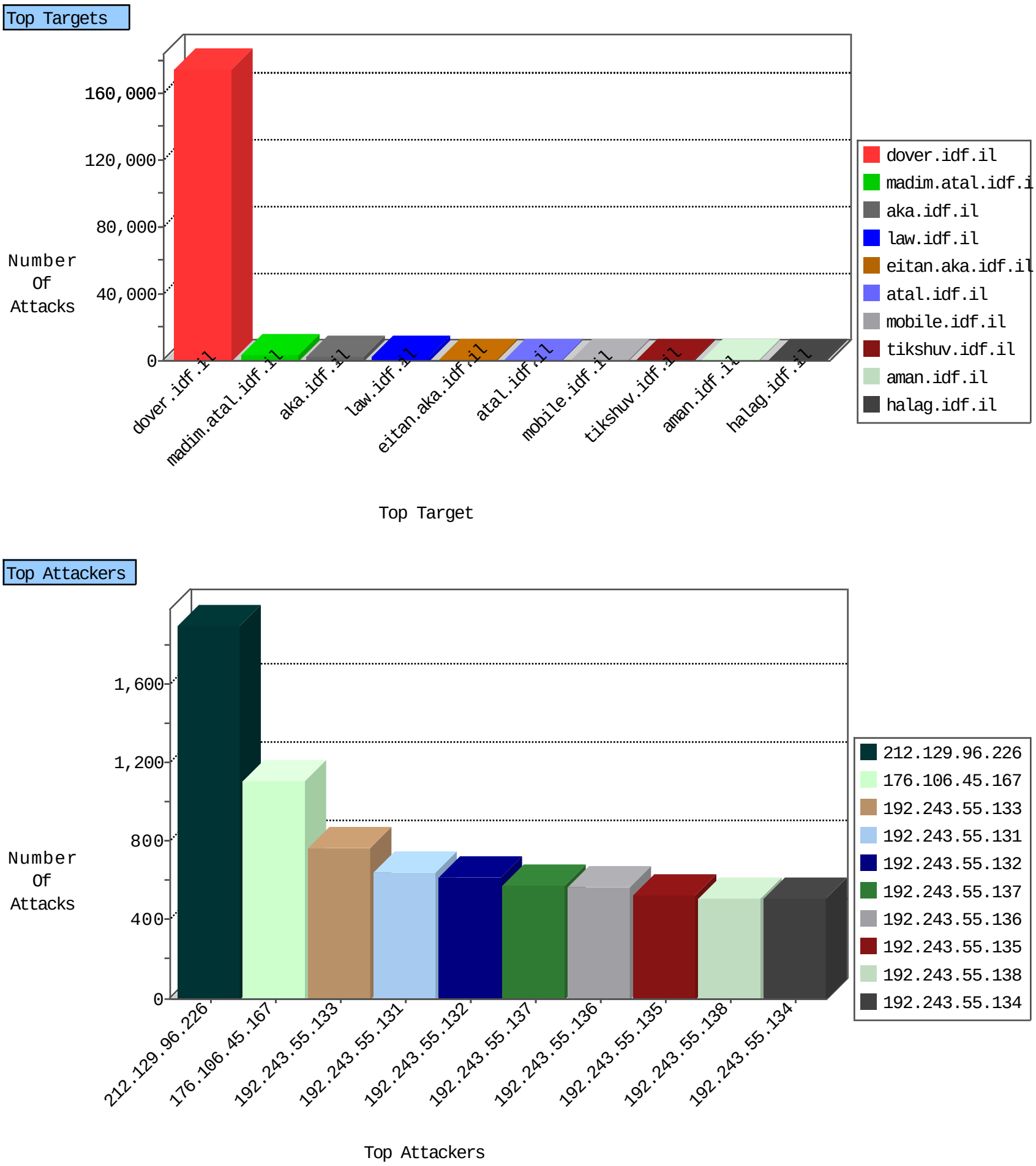
03-04-2016 to 03-05-2016

IDF Under Attack Daily Report



03-04-2016 to 03-05-2016

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	1200237
201.84.28.208	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41246
160.246.202.240	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41038
222.33.254.102	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40791
117.31.68.105	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	39317
142.134.240.56	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	38449
137.50.19.131	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37944
208.116.216.180	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37893
212.121.213.170	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37874
69.227.253.235	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37807
38.30.154.106	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37147
59.155.69.159	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36262
155.172.227.228	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36061
15.167.11.129	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35961
118.75.183.57	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35712
157.218.110.138	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35703
159.54.100.242	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35630
248.224.238.101		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35380
76.233.198.156	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35329
0.54.120.236		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35150
145.123.253.203	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35130
10.191.18.34		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34958
134.184.150.226	Belgium	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34840
212.117.243.46	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34634
122.198.39.111	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34387
206.154.154.198	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34297
10.174.32.5		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34204
34.165.221.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34157
57.208.12.50	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34092
92.142.71.44	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34008
111.155.113.39	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33933
6.255.244.130	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33932
157.227.5.18	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33923
105.100.58.10	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33909
128.199.129.168	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33880
239.8.209.40		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33872
20.70.149.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33864
246.193.156.219		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33822
164.95.183.241	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33817
39.120.30.171	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33807
33.224.233.28	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33749
79.218.89.56	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33741
254.3.40.164		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33738
146.128.154.117	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33735
99.19.46.66	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33715
193.90.47.24	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33708
177.42.156.105	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33684
157.129.20.38	Finland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33682
81.11.221.249	Belgium	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33674
178.121.31.27	Belarus	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33665

03-04-2016 to 03-05-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
79.182.173.24	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	23
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
123.126.113.162	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
61.135.189.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	18
79.182.151.228	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
31.168.82.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
46.116.11.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
79.181.51.90	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
87.68.251.254	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
85.64.4.23	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
5.22.135.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
37.142.233.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
31.154.154.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.103.124	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.177.217.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
82.102.136.66	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
109.253.159.88	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	7
46.19.86.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.93.101	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
89.138.94.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
104.236.37.53		147.237.72.166	aka.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	6
109.64.252.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.65.32.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
212.179.42.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
217.132.131.244	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	5
66.249.93.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.93.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
79.179.32.215	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
37.26.149.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.181.149.106	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
85.250.86.43	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
151.80.31.154	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	4
2.54.188.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
5.9.111.70	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	3
151.80.31.153	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	3
185.106.92.164		147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	3
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
213.57.220.233	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
2.54.23.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.54.41.51	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.9.111.70	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
5.29.89.174	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2

03-04-2016 to 03-05-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	94
24.104.233.195	147.237.77.216	United States	dover.idf.il	GPL SCAN nmap TCP	40
80.246.130.5	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	12
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
185.99.32.3	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sA (2)	8
66.249.64.153	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	6
185.32.179.90	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	5
80.246.133.16	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
118.200.0.245	147.237.76.197	Singapore	e.himush.idf.il	ET SCAN Potential SSH Scan	3
58.61.199.134	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	2
82.80.25.144	147.237.76.31	Israel	nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.102.9.28	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
64.233.172.171	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.27	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
42.203.50.219	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	2
119.188.4.9	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.65	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.34	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	2
66.102.9.6	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
37.8.118.211	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
40.117.92.242	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 3072	2
68.180.228.112	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
82.80.25.144	147.237.0.200	Israel	m4u.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.184	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
58.61.199.134	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
119.164.254.57	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	2
82.80.25.144	147.237.77.227	Israel	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.25	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.193	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
159.122.220.108	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
112.33.3.69	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	147.237.76.198	Israel	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
186.208.65.232	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.114.117.177	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.185	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
41.169.77.218	147.237.77.170	South Africa	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
177.158.19.243	147.237.76.177	Brazil	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
185.72.179.221	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1
118.200.0.245	147.237.76.147	Singapore	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
85.65.161.188	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
213.136.91.26	147.237.76.86	Germany	navy.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.0.15	Latvia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

03-04-2016 to 03-05-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	308
62.219.47.251	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	201
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	171
5.29.212.105	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	139
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	133
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	121
109.64.181.31	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
84.109.204.64	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	111
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	109
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	108
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	102
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	101
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	99
109.253.135.224	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	96
185.3.147.208	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	95
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	93
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	92
176.106.45.167	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	86
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	86
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	86
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	85
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	83
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	81
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	80
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	79
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
49.246.230.40	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	75
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	75
2.54.169.16	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	68
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	67
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	67
46.135.126.4	Czech Republic	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	67
176.13.17.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	65
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	65
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	64
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	64
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	63
87.69.33.78	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	61
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	61
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	60
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	58
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	57
83.14.142.130	Poland	147.237.77.216	dover.idf.il	drop	SAM rule	drop	57

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	319
2.54.23.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	317
31.154.151.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	287
84.228.116.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	274
2.54.42.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	265
185.32.179.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	170
109.67.3.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	168
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
79.182.221.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
2.54.41.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
109.67.52.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
85.64.244.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
149.78.204.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
213.57.208.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
37.26.147.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
2.52.151.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	38
79.183.151.9	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.183.151.9	Block	25
109.65.39.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
109.253.206.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	23
109.253.133.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
79.181.220.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
149.78.22.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
2.54.10.65	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.10.65	Block	19
2.54.129.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
176.13.2.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
109.253.136.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
37.142.64.28	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	11
87.68.240.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
176.13.21.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
213.57.200.23	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.200.23	Block	10
185.32.179.206	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	10
37.26.149.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
185.3.147.122	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	9
176.13.7.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
79.179.23.197	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 79.179.23.197	None	8
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	8
46.120.147.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	8
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	7
66.249.84.165	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	7