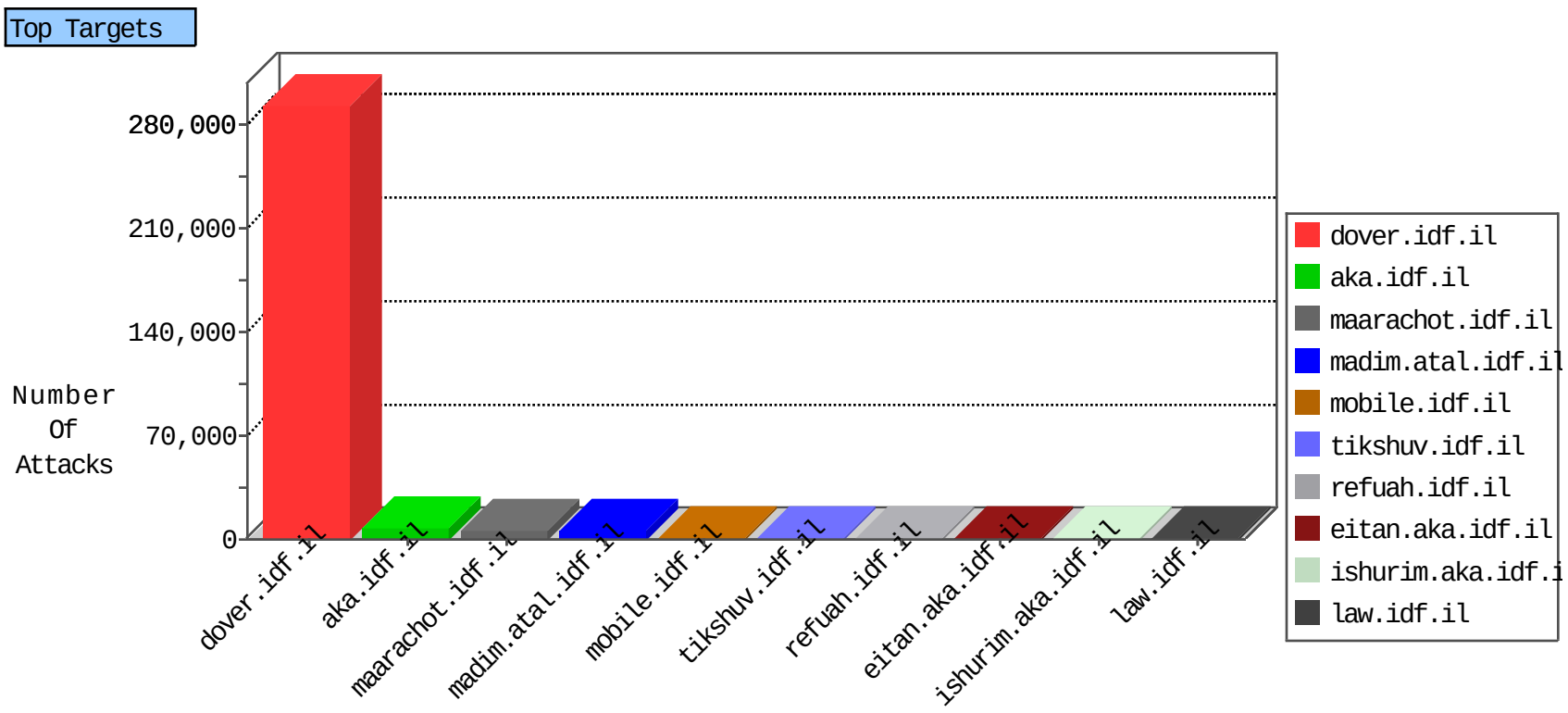
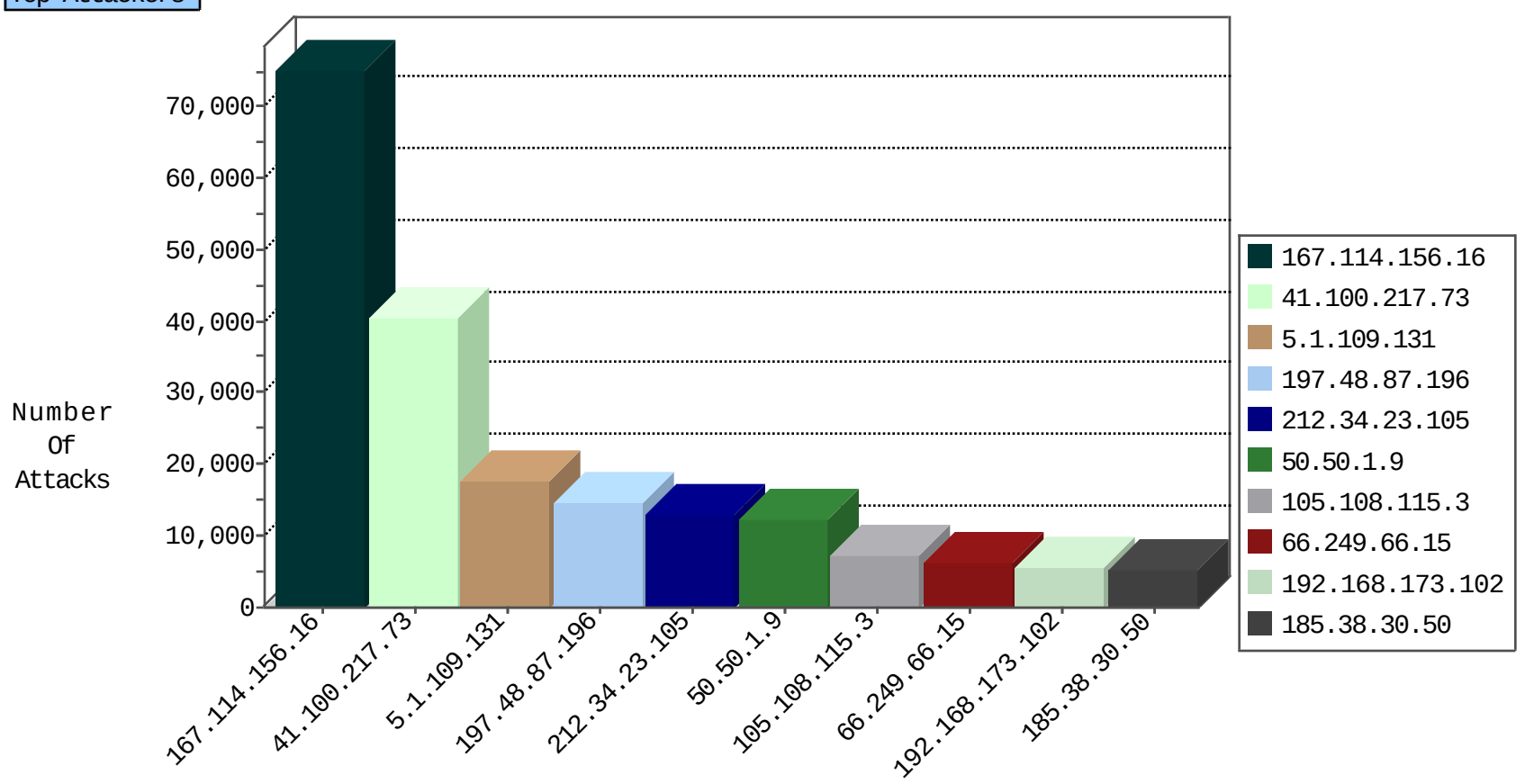
04-07-2016 to 04-08-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-07-2016 to 04-08-2016

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.i	HTTP Page Flood Attack	forward	887676
212.34.23.105	Jordan	147.237.77.216	dover.idf.i	HTTP Page Flood Attack	forward	478806
31.171.244.115	Switzerland	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	226005
37.239.68.65	Iraq	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	116038
41.238.1.239	Egypt	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	112833
167.114.156.16	Canada	147.237.77.216	dover.idf.i	Block_Ip_Web_In	drop	75286
41.254.2.247	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	67118
174.100.40.155	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	56513
212.34.23.105	Jordan	147.237.77.216	dover.idf.i	DOS-HTTP-fireflood	dest-reset	56070
37.239.68.61	Iraq	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	44152
212.179.212.111	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	38364
105.158.131.4	Morocco	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	38252
23.27.13.48	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	25210
192.117.105.2	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	21842
182.140.230.15	China	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	20091
2.54.140.193	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	19965
41.100.217.73	Algeria	147.237.77.216	dover.idf.i	HTTP Page Flood Attack	forward	12937
212.143.142.56	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	12036
212.34.23.105	Jordan	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	11823
37.26.146.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	9456
87.70.21.10	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	6439
74.73.166.84	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	4739
92.241.50.37	Jordan	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	4658
41.100.217.73	Algeria	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	4017
46.19.85.24	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3843
41.100.217.73	Algeria	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	3826
105.103.157.122	Algeria	147.237.77.216	dover.idf.i	HTTP-MISC-DoS-GoodBye-30	dest-reset	3497
2.54.177.167	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3486
41.231.217.18	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3173
41.108.45.145	Algeria	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3137
79.183.141.183	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2853
41.140.130.84	Morocco	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2680
37.239.68.12	Iraq	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2673
66.249.64.153	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2565
149.78.154.69	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2537
89.238.143.70	United Kingdom	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2506
207.159.160.150	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2370
197.211.52.22	Nigeria	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2332
93.172.184.124	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2241
95.186.83.130	Saudi Arabia	147.237.77.216	dover.idf.i	DOS-Tool-SwitchbladG	dest-reset	2085
141.255.153.16	Netherlands	147.237.77.216	dover.idf.i	DOS-Tool-SwitchbladG	dest-reset	1988
87.71.61.125	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1968
93.63.226.141	Italy	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1796
212.34.23.105	Jordan	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	1786
50.50.1.9	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1756
167.114.156.16	Canada	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1645
212.179.21.194	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1502
37.8.12.80	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	1330
197.8.36.51	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1062
197.1.145.78	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1015

04-07-2016 to 04-08-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.112.43.151	Korea, Republic of	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	120
41.44.188.168	Egypt	147.237.77.216	dover.idf.il	20034: HTTP: HOIC Denial-of-Service Tool Usage	Block	92
197.2.214.44	Tunisia	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	77
84.111.234.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	41
46.19.85.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	38
213.57.154.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	28
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
87.69.130.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	24
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
84.108.240.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
185.3.147.159	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	16
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	C1000064: HTTP: Access to - admin.asp	Block	14
132.66.62.239	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
91.197.61.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
84.109.232.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
109.65.81.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.181.108.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
109.253.130.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
2.55.33.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.109.24.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
149.78.150.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
149.78.168.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
196.184.62.248	Tunisia	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	10
105.104.90.16	Algeria	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	9
109.67.22.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
66.135.63.82	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
46.121.111.247	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.177.241.133	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.183.182.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.8.204.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.57.45.108	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.240.151	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.253.213.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
77.125.129.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
161.202.65.121	Japan	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	7
213.8.204.29	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
85.64.109.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.28.137.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
85.64.202.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.133.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
185.130.5.208	Lithuania	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
157.55.39.113	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
84.228.243.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
184.168.193.34	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
82.165.24.123	Germany	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
62.90.2.157	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
64.31.44.6	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-07-2016 to 04-08-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	6264
66.249.69.92	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	284
66.249.79.185	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	224
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	73
46.19.85.227	147.237.0.34	Israel	tikshuv.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	48
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	46
2.54.172.35	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
197.5.22.6	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP login.htm access	19
197.5.22.6	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP adminlogin access	14
82.165.24.123	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	14
66.135.63.82	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
66.102.8.182	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	10
184.168.193.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	9
63.143.34.37	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	8
212.34.23.105	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	7
74.63.228.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
105.104.90.16	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP admin.php access	6
213.246.49.97	147.237.77.74	France	law.idf.il	SQL Injection - Select From	6
64.31.44.6	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
105.104.90.16	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP login.htm access	5
173.255.233.124	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
66.249.79.172	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	5
197.2.105.86	147.237.76.39	Tunisia	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	4
176.13.2.107	147.237.0.19	Israel	madim.atal.idf.il	GPL SCAN myscan	4
41.254.2.80	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string	4
176.13.2.107	147.237.0.19	Israel	madim.atal.idf.il	INDICATOR-SCAN myscan	4
197.5.22.6	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP admin.php access	4
196.203.238.161	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP admin.php access	3
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	3
197.2.105.86	147.237.76.44	Tunisia	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
196.203.238.161	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP login.htm access	3
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
197.2.105.86	147.237.76.34	Tunisia	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
66.249.65.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	3
197.2.105.86	147.237.76.30	Tunisia	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
82.102.202.9	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	3
105.104.90.16	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP adminlogin access	3
173.255.233.124	147.237.77.216	United States	dover.idf.il	GPL WEB_SERVER TRACE attempt	2
87.139.236.153	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
80.246.133.255	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
87.139.236.153	147.237.8.28	Germany	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
94.200.77.62	147.237.77.212	United Arab Emirates	e.dover.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
94.200.77.62	147.237.77.170	United Arab Emirates	maarachot.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
94.200.77.62	147.237.76.200	United Arab Emirates	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
80.82.78.38	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	2
87.71.18.95	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN NMAP -sA (2)	2
197.2.105.86	147.237.76.31	Tunisia	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2

04-07-2016 to 04-08-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.100.217.73	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34327
50.50.1.9	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12286
5.1.109.131	Iraq	147.237.77.216	dover.idf.i	Block HTTP Non Compliant	Response out of state	monitor	11298
105.108.115.3	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7301
197.48.87.196	Egypt	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	5485
185.38.30.50	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5102
197.48.87.196	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4571
5.1.109.131	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4007
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3918
197.6.241.141	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3734
192.168.173.102		147.237.77.216	dover.idf.i	Geo-location enforcement	Geo-location inbound enforcement	monitor	3504
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3290
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3233
41.254.8.34	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3169
5.1.106.127	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3114
197.48.87.196	Egypt	147.237.77.216	dover.idf.i	drop		drop	2792
41.254.9.131	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2787
95.213.193.102	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2665
41.254.2.247	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2614
156.197.238.111	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2459
50.50.1.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2450
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	2033
105.158.161.46	Morocco	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1814
197.0.178.136	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1760
41.254.9.15	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	drop	SAM rule	drop	1660
156.196.81.152	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1643
149.200.147.7	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1627
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1586
37.8.12.80	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1399
41.254.6.60	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1336
41.254.2.247	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	drop		drop	1176
207.232.28.242	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	968
41.254.9.15	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	897
141.255.153.16	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	896
212.126.112.38	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	814
5.1.109.131	Iraq	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	788
156.197.72.53	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	778
41.100.217.73	Algeria	147.237.77.216	dover.idf.i	drop		drop	767
94.249.90.145	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	725
5.1.109.131	Iraq	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	642
15.203.169.107	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	586
185.120.125.67	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	583
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	562
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	541
46.32.127.152	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	527
45.244.108.162	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	491
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	461
156.196.221.133	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	457
197.48.87.196	Egypt	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	440
197.48.87.196	Egypt	147.237.77.216	dover.idf.i	Bad TCP sequence		monitor	414

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.142.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	319
188.120.152.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	269
109.253.200.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	258
41.254.8.34	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.254.8.34	Block	224
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	222
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	190
149.88.135.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	179
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.5.22.6	Block	174
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	165
185.32.179.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	154
109.253.202.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	150
46.19.85.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	148
109.253.138.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	144
2.53.3.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
95.213.193.102	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.213.193.102	Block	124
176.13.13.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
87.70.8.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.120.142.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.53.36.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
2.55.10.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
80.246.136.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
80.246.136.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
109.253.221.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
2.52.164.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
176.13.2.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
109.253.132.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
79.180.36.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
149.78.175.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
2.53.59.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
109.253.143.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
109.253.131.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	65
46.19.85.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
176.13.21.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
84.228.213.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
46.19.85.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
105.104.90.16	Algeria	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	63
2.53.38.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
109.253.203.154	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter RepeatPassword	Block	62
105.104.90.16	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.104.90.16	Block	61
85.64.115.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
2.54.162.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
2.52.168.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53

04-07-2016 to 04-08-2016