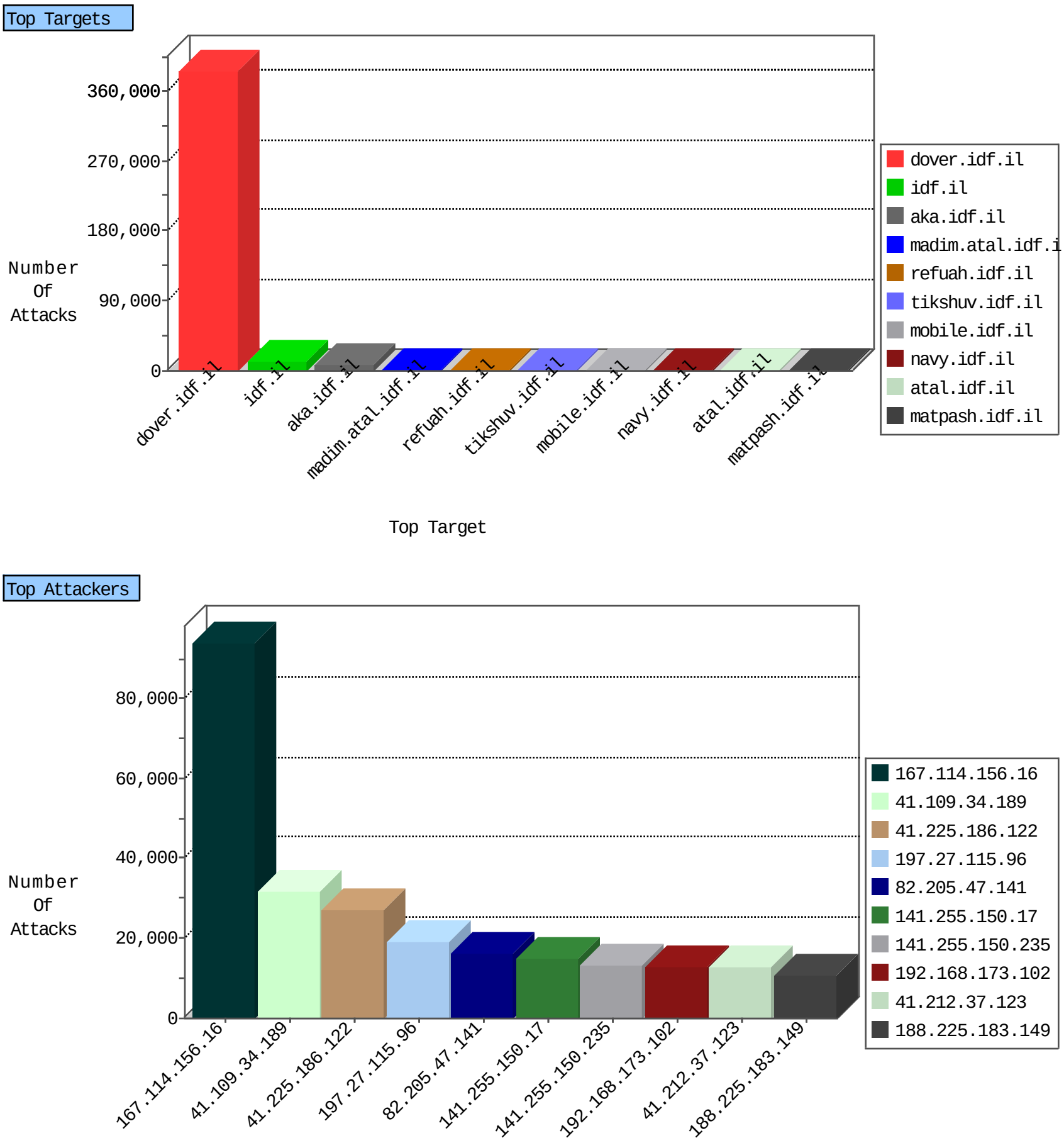
04-09-2016 to 04-10-2016

IDF Under Attack Daily Report



04-09-2016 to 04-10-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.i	Block_Ip_Web_In	drop	94144
141.255.159.119	Netherlands	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	57054
0.0.0.0		147.237.77.216	dover.idf.i	HTTP Page Flood Attack	forward	44643
0.0.0.0		147.237.77.216	dover.idf.i	HTTP-POST-Segmented-DoS	dest-reset	30526
212.143.142.56	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	18216
197.0.254.101	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	17829
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	16477
36.71.23.100	Indonesia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	10850
196.206.9.35	Morocco	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	9050
90.231.228.209	Sweden	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	8845
194.150.168.79	Germany	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	8441
46.19.85.94	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	7301
156.203.4.82	Egypt	147.237.77.216	dover.idf.i	HTTP-POST-Segmented-DoS	dest-reset	6644
156.203.99.213	Egypt	147.237.77.216	dover.idf.i	HTTP-POST-Segmented-DoS	dest-reset	6112
41.230.102.88	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	4605
141.255.146.128	Netherlands	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	4568
105.157.207.129	Morocco	147.237.77.216	dover.idf.i	DOS-WEB-HULK-improved	forward	4218
105.110.11.17	Algeria	147.237.77.216	dover.idf.i	DOS-HTTP-fireflood	dest-reset	3963
65.19.167.131	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3841
46.19.85.79	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3782
176.10.104.243	Switzerland	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3653
128.177.133.102	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3591
93.115.95.205	Anonymous Proxy	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3539
216.17.101.79	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3488
80.255.4.76	Germany	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3414
181.54.81.104	Colombia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3293
37.106.143.122	Saudi Arabia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3217
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3141
46.19.85.115	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2983
197.16.135.221	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2941
85.114.116.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2903
105.157.81.32	Morocco	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2633
117.220.123.207	India	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2608
197.27.76.241	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2258
197.7.198.64	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2036
141.255.156.106	Netherlands	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1936
197.27.115.96	Tunisia	147.237.77.216	dover.idf.i	DOS-HTTP-fireflood	dest-reset	1730
41.232.63.102	Egypt	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1725
95.145.28.178	United Kingdom	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1711
197.0.79.194	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1617
38.130.96.253	United States	147.237.77.216	dover.idf.i	HTTP-POST-Segmented-DoS	dest-reset	1556
141.255.150.17	Netherlands	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	1530
197.1.123.225	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1472
41.251.130.235	Morocco	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1453
66.249.83.155	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1424
31.154.173.237	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1243
178.39.218.11	Switzerland	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1213
41.111.2.130	Algeria	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	1187
144.76.4.148	Germany	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1102
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1058

04-09-2016 to 04-10-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	41
109.107.233.15	Jordan	147.237.77.216	dover.idf.il	C1000064: HTTP: Access to - admin.asp	Block	30
106.120.173.85	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	20
61.135.189.99	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	17
82.81.21.195	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
84.108.68.54	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	13
79.180.7.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
5.134.114.87	Spain	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	12
79.176.72.189	Israel	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	12
207.232.46.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
80.255.4.76	Germany	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	12
46.19.86.81	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
79.183.230.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	10
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	10
107.168.70.85	Japan	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	9
123.126.113.167	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	9
93.63.188.181	Italy	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
216.201.148.210	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
109.67.62.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.108.75.224	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.64.223.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
188.120.148.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
64.31.44.6	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
197.7.198.64	Tunisia	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	6
79.179.117.100	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
89.138.39.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.66.59	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
77.125.90.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
64.31.44.6	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
74.208.133.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.70.84.112	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
174.34.135.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
82.165.24.123	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
158.85.253.245	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
109.65.215.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
144.76.61.21	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
91.219.122.4	Poland	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
79.180.192.113	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
149.50.59.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
103.21.58.191	India	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.71.37.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
207.46.13.45	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
93.63.188.181	Italy	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
84.245.33.104	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
107.168.70.162	Japan	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	4

04-09-2016 to 04-10-2016

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	90
82.205.47.141	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	72
109.107.233.15	147.237.77.216	Jordan	dover.idf.il	Admin login page scan - Havij	48
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	30
213.247.63.11	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	24
64.31.44.6	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	14
74.84.136.105	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	12
90.231.228.209	147.237.77.216	Sweden	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	12
23.91.70.121	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
103.21.58.191	147.237.77.74	India	law.idf.il	SQL Injection - Select From	12
93.63.188.181	147.237.77.233	Italy	atal.idf.il	SQL Injection - Select From	12
216.201.148.210	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
70.89.127.77	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	9
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	8
93.63.188.181	147.237.76.42	Italy	refuah.idf.il	SQL Injection - Select From	8
109.107.233.15	147.237.77.216	Jordan	dover.idf.il	SERVER-WEBAPP admin.php access	6
87.242.112.35	147.237.72.166	Russian Federation	aka.idf.il	SQL Injection - Select From	6
23.91.70.119	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	6
84.245.33.104	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	6
202.124.109.87	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	6
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
82.165.24.123	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	6
74.208.133.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
91.219.122.4	147.237.77.233	Poland	atal.idf.il	SQL Injection - Select From	6
74.63.228.226	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
109.107.233.15	147.237.77.216	Jordan	dover.idf.il	SERVER-WEBAPP adminlogin access	5
82.205.111.236	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	4
109.107.233.15	147.237.77.216	Jordan	dover.idf.il	SERVER-WEBAPP login.htm access	4
177.185.194.45	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	4
37.187.34.14	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
82.166.118.226	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
70.89.127.78	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
178.62.96.169	147.237.77.216	United Kingdom	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	3
37.26.149.146	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
174.37.194.144	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sA (2)	2
82.205.47.141	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
208.100.26.228	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	2
156.203.99.213	147.237.77.216	Egypt	dover.idf.il	ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string	2
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
66.249.65.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
80.82.78.38	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
41.107.31.16	147.237.77.216	Algeria	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
79.177.68.191	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
208.100.26.228	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
46.60.17.32	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
208.100.26.228	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
64.233.172.163	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
84.111.152.251	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2

04-09-2016 to 04-10-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.205.47.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14193
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13333
141.255.150.235	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13200
141.255.150.17	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12848
41.212.37.123	Kenya	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12552
197.27.115.96	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11936
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10955
188.225.183.149	Palestinian Territory, Occupied	147.237.0.33	idf.il	drop		drop	10903
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	Bad TCP sequence		monitor	10555
192.168.173.102		147.237.77.216	dover.idf.i	Geo-location enforcement	Geo-location inbound enforcement	monitor	8581
141.255.156.147	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8170
41.100.50.133	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8039
197.1.123.225	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7472
212.106.79.2	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6642
141.255.159.119	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6618
197.27.115.96	Tunisia	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	6329
105.110.11.17	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4438
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	4435
141.255.156.106	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3877
46.165.221.230	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3372
193.90.12.88	Norway	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3234
105.157.207.129	Morocco	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3118
185.129.62.63	Denmark	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3051
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	2983
88.200.73.100	Slovenia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2785
94.249.51.221	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2522
38.130.96.253	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2336
141.255.146.128	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2101
37.237.140.107	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1816
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	drop		drop	1599
65.19.167.130	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1539
38.130.96.253	United States	147.237.77.216	dover.idf.i	Bad TCP sequence		monitor	1530
37.26.147.150	Israel	147.237.77.216	dover.idf.i	drop	SAM rule	drop	1530
46.185.244.209	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1528
216.17.101.79	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1495
178.175.128.50	Moldova, Republic of	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1334
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1245
18.248.1.85	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1119
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	drop		drop	1112
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1110
195.154.56.44	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1093
173.245.66.142	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1035
146.185.177.103	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	993
17.138.56.13	United States	147.237.77.216	dover.idf.i	drop	SAM rule	drop	969
37.238.144.63	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	963
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	alert	825
192.42.116.16	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	814
194.150.168.79	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	787
17.138.56.13	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	743
85.93.218.204	Luxembourg	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	715

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.248	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2151
37.26.147.248	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 37.26.147.248	Block	2150
37.26.147.248	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 37.26.147.248	Block	2150
37.26.147.150	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1252
37.26.147.150	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1252
37.26.147.150	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1252
185.27.105.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	332
109.107.233.15	Jordan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.107.233.15	Block	297
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	186
105.157.207.129	Morocco	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Value from 105.157.207.129	Block	148
37.26.149.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
109.253.202.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
46.19.86.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
109.107.233.15	Jordan	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 109.107.233.15	Block	95
109.107.233.15	Jordan	147.237.77.216	dover.idf.il	PHP Attempt	Block	86
89.139.140.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.139.140.29	Block	70
2.53.60.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
82.205.47.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Automated Vulnerability Scanning V1	Block	50
105.157.207.129	Morocco	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Query String from 105.157.207.129	Block	44
79.180.167.112	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.180.167.112	Block	38
46.19.86.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
2.53.22.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
37.26.147.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
175.43.95.152	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.43.95.152	Block	29
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 156.203.99.213	Block	28
105.157.207.129	Morocco	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Parameter Name from 105.157.207.129	Block	27
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
79.180.167.112	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	25
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	Multiple Malformed URL from 156.203.99.213	Block	25
37.26.148.202	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	24
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	24
37.26.147.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
105.157.207.129	Morocco	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 105.157.207.129	Block	18
37.58.52.30	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.58.52.30	Block	12
41.251.130.235	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.251.130.235	Block	12
79.180.167.112	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	10
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	10
109.64.88.236	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.88.236	Block	9
77.127.2.50	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	9
185.120.125.3	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	8
81.218.116.129	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	8
149.78.23.55	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.23.55	Block	7
77.127.2.50	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.127.2.50	Block	7
41.107.31.16	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.107.31.16	Block	7
80.84.1.10	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
192.40.95.10	Finland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.40.95.10	Block	7
109.65.49.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
5.44.169.128	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
185.120.125.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6