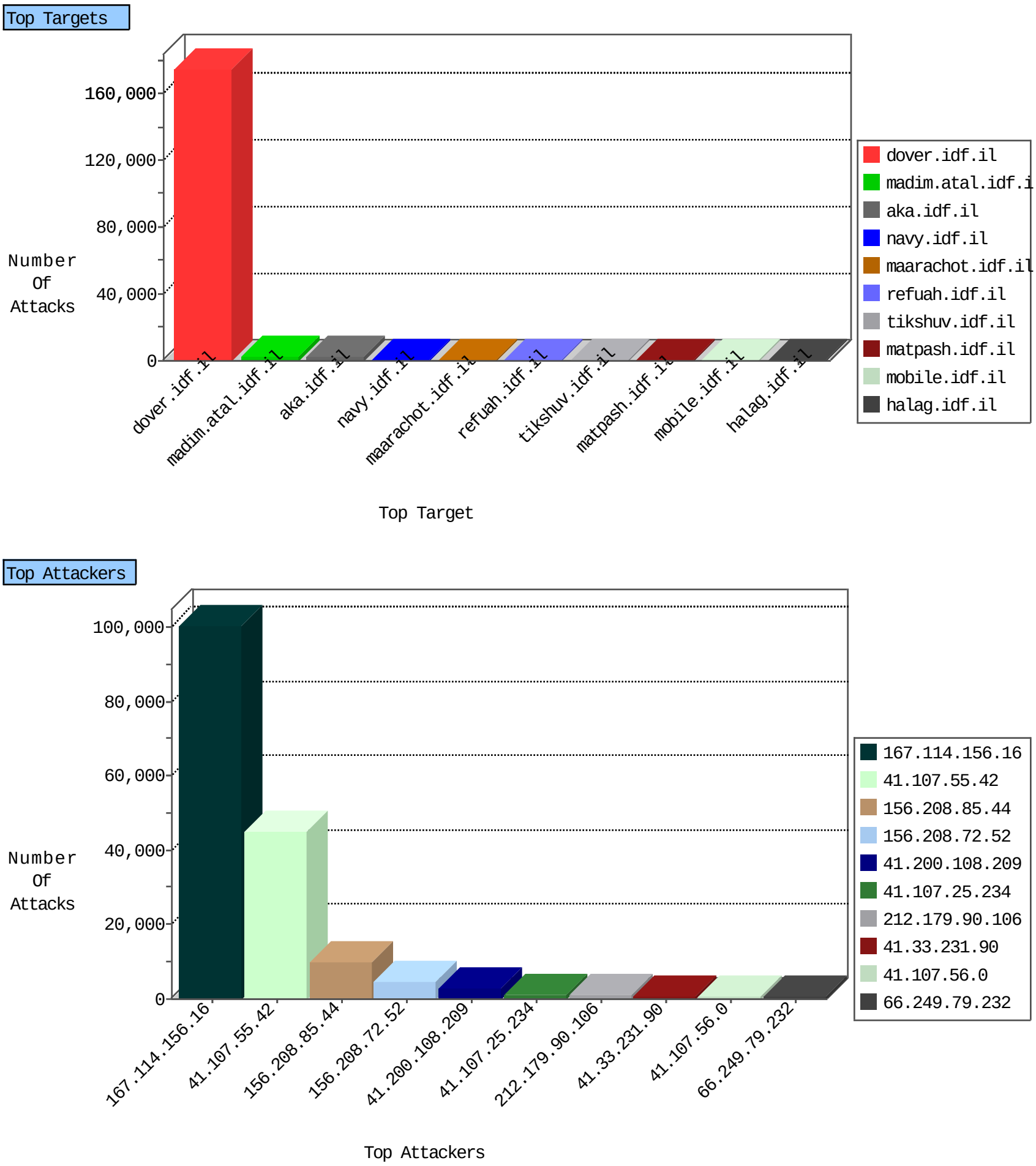
04-16-2016 to 04-17-2016

IDF Under Attack Daily Report



04-16-2016 to 04-17-2016

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.il	Block_Ip_Web_In	drop	100598
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8055
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5810
41.200.108.209	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2920
105.155.246.141	Morocco	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	614
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	601
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	452
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	302
41.200.108.209	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	286
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	44
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	27
41.107.56.0	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	26
41.107.63.148	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	26
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	18
14.175.168.54	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	17
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	14
79.179.224.72	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
82.80.230.228	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.182.16.12	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
109.64.163.186	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	5
109.66.70.248	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
105.155.246.141	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	4
120.132.50.135	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	4
82.145.208.202	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	4
123.59.59.52	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	4
79.178.205.207	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
77.41.88.44	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
37.204.142.237	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
8.37.227.124	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
188.138.17.205	France	147.237.77.74	law.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
185.70.184.164	Netherlands	147.237.72.14	dover.idf.il(old)	JLM_Under_Attack_Con_Https	drop	2
101.201.147.32	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
82.145.220.9	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	2
216.249.107.200	United States	147.237.72.166	aka.idf.il	Anomaly-TCP-shortheader	dest-reset	2
124.107.243.130	Philippines	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
77.41.88.44	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.204.142.237	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
101.201.147.32	China	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
82.145.223.22	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	2
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
8.37.227.124	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2

04-16-2016 to 04-17-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	41
106.120.173.139	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	25
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
98.19.222.133	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	24
109.64.153.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	23
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
84.111.122.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
98.19.222.133	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
5.28.156.130	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.179.16.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
66.76.174.2	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
103.3.173.97	Malaysia	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
158.85.253.245	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.173.233.226	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
79.178.102.17	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.78.161.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.178.0.28	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.178.223.238	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.112.235	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.108.246.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.5.182	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
87.242.112.35	Russian Federation	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
106.120.173.124	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
2.53.159.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
5.102.242.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.70.98.59	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.179.125.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.180.139.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
85.250.163.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
194.88.154.138	Poland	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
209.15.196.171	Canada	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.89.19.29	Turkey	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.67.169.124	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
194.88.154.138	Poland	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
184.173.233.226	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
209.15.196.171	Canada	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
79.178.102.11	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
144.76.93.46	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
87.242.112.35	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.175.157.102	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
84.245.33.104	Netherlands	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.246.49.97	France	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
64.87.23.55	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.242.112.35	Russian Federation	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4

04-16-2016 to 04-17-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.232	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	642
66.249.66.60	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	343
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	96
98.19.222.133	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	94
46.19.85.164	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	48
46.19.85.61	147.237.77.176	Israel	matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	44
66.76.174.2	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	36
194.88.154.138	147.237.76.86	Poland	navy.idf.il	SQL Injection - Select From	28
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	26
103.3.173.97	147.237.77.233	Malaysia	atal.idf.il	SQL Injection - Select From	24
79.177.194.11	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	22
87.242.112.35	147.237.77.176	Russian Federation	matpash.idf.il	SQL Injection - Select From	22
79.177.26.44	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	18
184.173.233.226	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	14
158.85.253.245	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	13
103.3.173.97	147.237.77.74	Malaysia	law.idf.il	SQL Injection - Select From	12
84.245.33.104	147.237.77.216	Netherlands	dover.idf.il	SQL Injection - Select From	10
209.15.196.171	147.237.76.86	Canada	navy.idf.il	SQL Injection - Select From	10
108.67.169.124	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
213.246.49.97	147.237.76.31	France	nakchal.idf.il	SQL Injection - Select From	9
87.71.107.113	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
177.185.194.45	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
64.87.23.55	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
108.175.157.102	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
87.242.112.35	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	6
93.89.19.29	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	6
216.249.107.200	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
185.32.179.212	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
89.248.167.131	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	3
95.45.254.123	147.237.72.166	Ireland	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
5.29.22.140	147.237.77.243	Israel	mobile.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.103	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
80.82.78.38	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
80.246.133.202	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
61.149.161.186	147.237.72.166	China	aka.idf.il	GPL SCAN nmap TCP	2
37.26.148.191	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
80.246.133.119	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.45.79.103	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
108.46.61.58	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
80.82.78.38	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
46.4.79.76	147.237.77.179	Germany	e.mazi.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
89.248.167.131	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
85.65.15.215	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
89.248.167.131	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	2
89.248.167.131	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.103	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	2

04-16-2016 to 04-17-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32788
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	drop		drop	3026
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2567
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2544
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	880
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	804
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	727
79.180.197.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	475
41.107.56.0	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	364
107.167.109.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	354
2.53.161.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	300
41.107.56.0	Algeria	147.237.77.216	dover.idf.il	drop		drop	295
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	261
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	251
109.67.55.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	221
80.246.133.202	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	214
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	199
41.107.25.234	Algeria	147.237.77.216	dover.idf.il	drop		drop	142
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	129
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	drop		drop	129
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	drop		drop	120
212.76.124.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
64.247.152.157	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
141.0.14.145	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
95.86.82.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
41.107.56.0	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	73
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
5.29.141.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	66
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	61
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	52
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	50
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
105.155.246.141	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
84.108.69.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
84.95.251.211	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
79.180.133.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
87.70.81.222	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
84.228.109.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
76.102.51.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.117.221.172	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
87.70.72.200	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 156.208.85.44	Block	1262
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 156.208.72.52	Block	1220
93.173.146.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	302
46.117.182.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	260
149.78.45.151	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	226
79.180.37.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	192
46.117.32.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	140
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
2.53.46.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
185.32.179.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
176.13.18.253	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	95
2.55.44.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
37.26.148.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
87.70.1.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
79.182.35.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
2.53.33.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
84.109.69.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
2.53.8.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	40
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
2.53.51.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
80.246.136.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
2.53.150.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	25
87.70.42.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
176.13.7.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
2.53.172.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
185.32.179.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
213.6.116.158	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 213.6.116.158	Block	13
2.55.133.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
64.79.85.205	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 64.79.85.205	Block	12
46.120.3.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
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	10
41.142.42.104	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.142.42.104	Block	10
185.120.126.111	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	9
109.67.136.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.13.11.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
54.227.3.234	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	8
54.161.63.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	8
79.177.21.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
185.3.147.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
54.159.214.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	7
54.145.224.236	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	7
185.120.126.111	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 185.120.126.111	Block	7
54.161.17.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	7
79.182.137.74	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.182.137.74	Block	7
46.120.212.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Multiple Malformed URL from 41.107.55.42	Block	6
54.163.158.202	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	6
2.53.37.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6