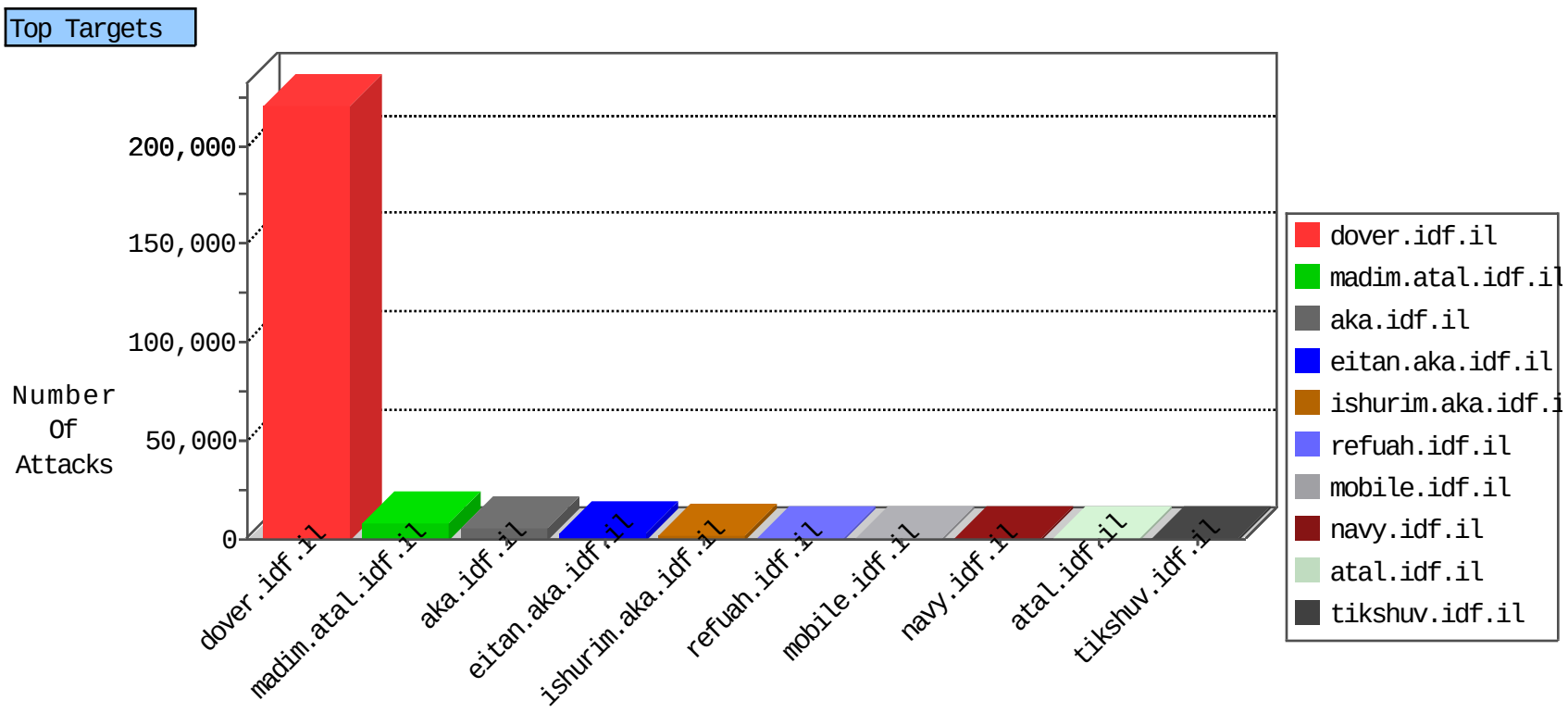
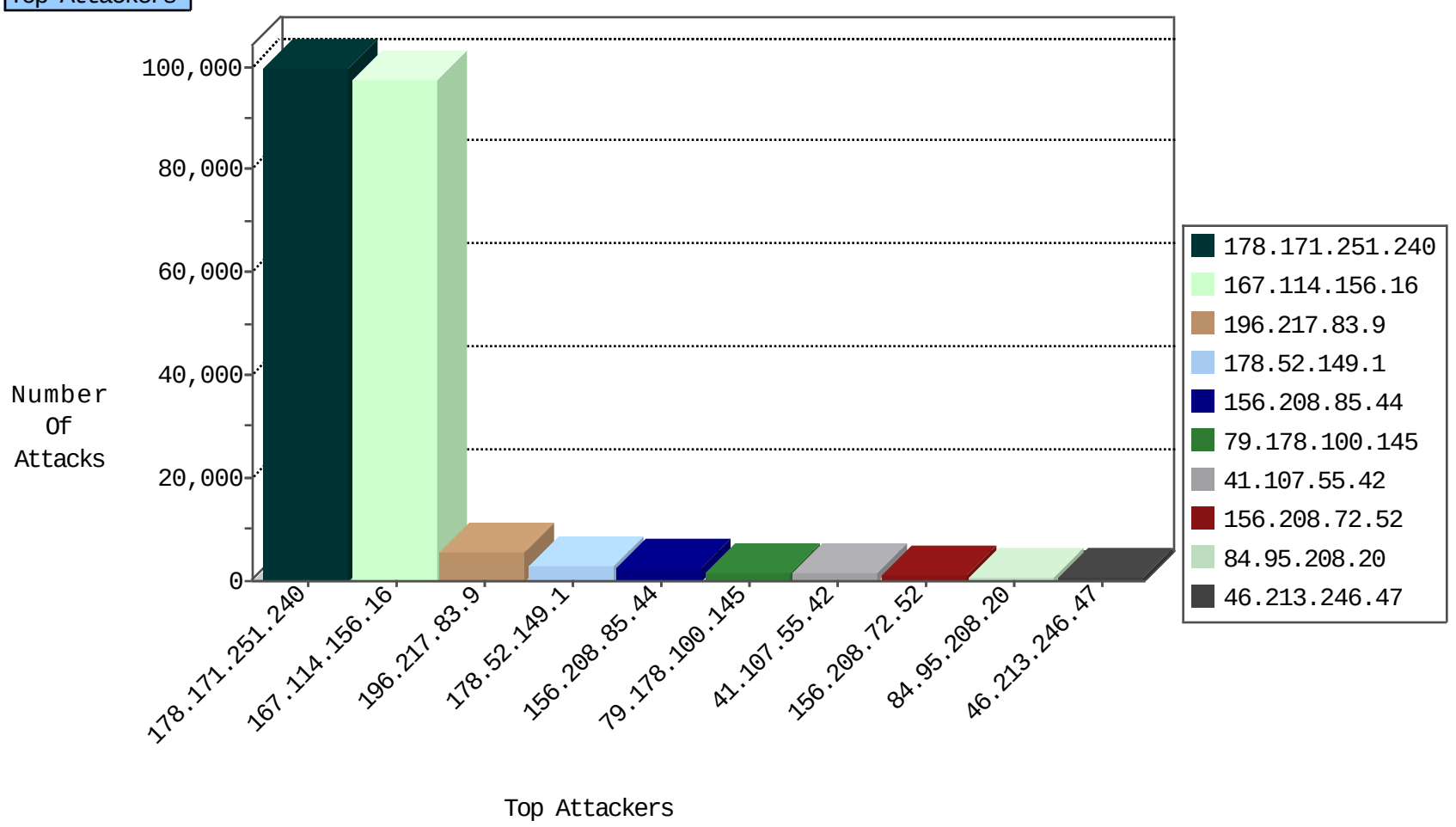
04-17-2016 to 04-18-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-17-2016 to 04-18-2016

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	97741
91.199.99.36	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2677
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2065
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1349
79.178.100.145	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1308
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1171
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	635
196.217.83.9	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	361
37.26.148.255	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	93
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
79.178.100.145	Israel	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	81
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	69
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	32
2.55.49.176	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	27
37.26.148.255	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
31.168.227.138	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
173.3.228.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
84.108.144.101	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	8
82.81.6.86	Israel	147.237.77.216	dover.idf.il	Invalid L4 Header Length	drop	7
167.220.196.89	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
82.81.6.86	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
79.182.173.17	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
79.183.119.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
196.218.61.220	Egypt	147.237.0.34	tikshuv.idf.il	L4 Source or Dest Port Zero	drop	6
123.59.59.52	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	4
120.132.50.135	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	4
93.174.93.218	Netherlands	147.237.72.166	aka.idf.il	block-sp-traf1	forward	4
123.59.59.52	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	4
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
141.0.14.144	Europe	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
95.25.14.10	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
188.138.75.133	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	3
84.108.85.95	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
104.148.71.133	United States	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	3
176.15.192.45	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.228.76	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
155.250.255.143	Germany	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
10.0.0.14		147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	3
212.179.228.76	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
95.86.92.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
176.77.32.221	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
180.153.235.242	China	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
155.250.255.140	Germany	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
95.86.98.189	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
80.74.96.29	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
188.138.75.133	Germany	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	2
202.112.51.96	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
101.201.147.32	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2

04-17-2016 to 04-18-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	21
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
84.95.88.77	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
84.111.39.32	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
106.120.173.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	17
213.57.136.20	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	14
79.177.54.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
5.28.144.175	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	12
87.70.90.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	11
37.142.72.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
31.210.186.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
89.138.222.32	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.116.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
66.96.128.60	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
2.53.20.22	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
188.120.157.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.178.167.88	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
59.120.255.127	Taiwan	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
79.181.51.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.57.205.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.64.165.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.94.180.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
188.120.148.34	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
213.57.33.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
89.138.191.241	Israel	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	6
109.65.6.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.57.161.231	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
2.53.7.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
80.246.133.167	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
93.89.19.29	Turkey	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
109.65.88.89	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
200.59.205.238	Argentina	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
134.119.5.86	Germany	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
195.234.228.90	Germany	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
81.218.145.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.45.65.196	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.192.77	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
70.89.127.78	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
149.88.198.104	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.135.63.82	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
87.71.122.45	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.1.67	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.53.146.216	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
136.243.5.87	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4

04-17-2016 to 04-18-2016

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	72
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	36
66.96.128.60	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	25
59.120.255.127	147.237.77.74	Taiwan	law.idf.il	SQL Injection - Select From	24
200.59.205.238	147.237.77.176	Argentina	matpash.idf.il	SQL Injection - Select From	23
79.177.192.128	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	13
177.185.192.77	147.237.0.34	Brazil	tikshuv.idf.il	SQL Injection - Select From	13
70.89.127.78	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	12
213.247.63.11	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	SQL Injection - Select From	12
152.115.70.227	147.237.76.86	Denmark	navy.idf.il	SQL Injection - Select From	12
70.89.127.78	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
177.185.192.98	147.237.77.216	Brazil	dover.idf.il	SQL Injection - Select From	12
177.185.192.77	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	11
66.249.93.44	147.237.76.31	Europe	nakchal.idf.il	ET SCAN NMAP -sA (2)	10
93.89.19.29	147.237.76.31	Turkey	nakchal.idf.il	SQL Injection - Select From	10
80.246.130.65	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
94.73.150.148	147.237.72.166	Turkey	aka.idf.il	SQL Injection - Select From	9
37.187.34.14	147.237.77.170	France	maarachot.idf.il	Tehila - Perl LWP with fake user agent	8
5.45.65.196	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	6
66.135.63.82	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
87.242.112.35	147.237.76.42	Russian Federation	refuah.idf.il	SQL Injection - Select From	6
177.185.192.50	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
23.91.70.77	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
89.138.191.241	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP login.htm access	5
93.89.19.29	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	5
195.234.228.90	147.237.77.216	Germany	dover.idf.il	SQL Injection - Select From	4
89.138.191.241	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP admin.php access	3
212.199.57.203	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
80.82.78.38	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
80.246.136.114	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
79.178.62.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.239	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	2
113.240.250.154	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.60	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
112.95.149.171	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
185.112.248.50	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	2
73.187.117.50	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	2
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
106.186.113.67	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
112.95.149.171	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.49	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.10	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
62.219.172.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.170.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
82.166.144.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.112.248.50	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential SSH Scan	1

04-17-2016 to 04-18-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	67680
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17601
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11516
196.217.83.9	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5146
178.52.149.1	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3063
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2429
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	679
46.213.246.47	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	586
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	493
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	334
109.67.174.18	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	300
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.179.59.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	285
79.182.173.17	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	273
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	232
196.217.83.9	Morocco	147.237.77.216	dover.idf.il	drop		drop	228
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	227
46.19.86.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
195.60.232.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	211
89.139.237.160	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	194
84.229.31.167	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	174
212.25.84.200	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	170
212.117.136.8	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	147
84.229.34.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
159.203.100.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
79.179.134.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	129
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
79.183.149.150	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack		reject	113
84.189.200.118	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
86.149.136.136	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
79.178.16.200	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	107
79.178.143.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	95
195.212.29.187	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
212.25.84.200	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	90
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	90
79.181.11.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
85.65.106.29	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
2.53.47.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
61.93.222.70	Hong Kong	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
213.99.33.158	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	64
213.99.33.158	Spain	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	64
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	64
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	62
207.241.229.102	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	60
128.69.170.170	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54

04-17-2016 to 04-18-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
176.13.3.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.209.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	368
109.253.156.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	309
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	300
2.53.142.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	241
46.19.85.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	233
80.246.136.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	199
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	194
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	187
2.53.27.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	183
2.53.144.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
176.13.15.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	171
46.19.85.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
109.253.157.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
46.19.85.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
80.246.137.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
185.32.179.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
2.53.167.162	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	129
84.94.68.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
80.246.136.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	125
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
89.138.191.241	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 89.138.191.241	Block	121
89.138.191.241	Israel	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 89.138.191.241	Block	115
176.13.19.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
46.19.86.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.53.62.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
176.13.10.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
2.55.38.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
185.32.179.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
2.53.19.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
109.253.194.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
80.246.136.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
2.53.15.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
46.19.86.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
80.246.136.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	89
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
37.26.148.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
176.13.7.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
109.253.143.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.253.200.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
109.253.128.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
109.253.204.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
213.8.204.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
80.246.137.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66

04-17-2016 to 04-18-2016