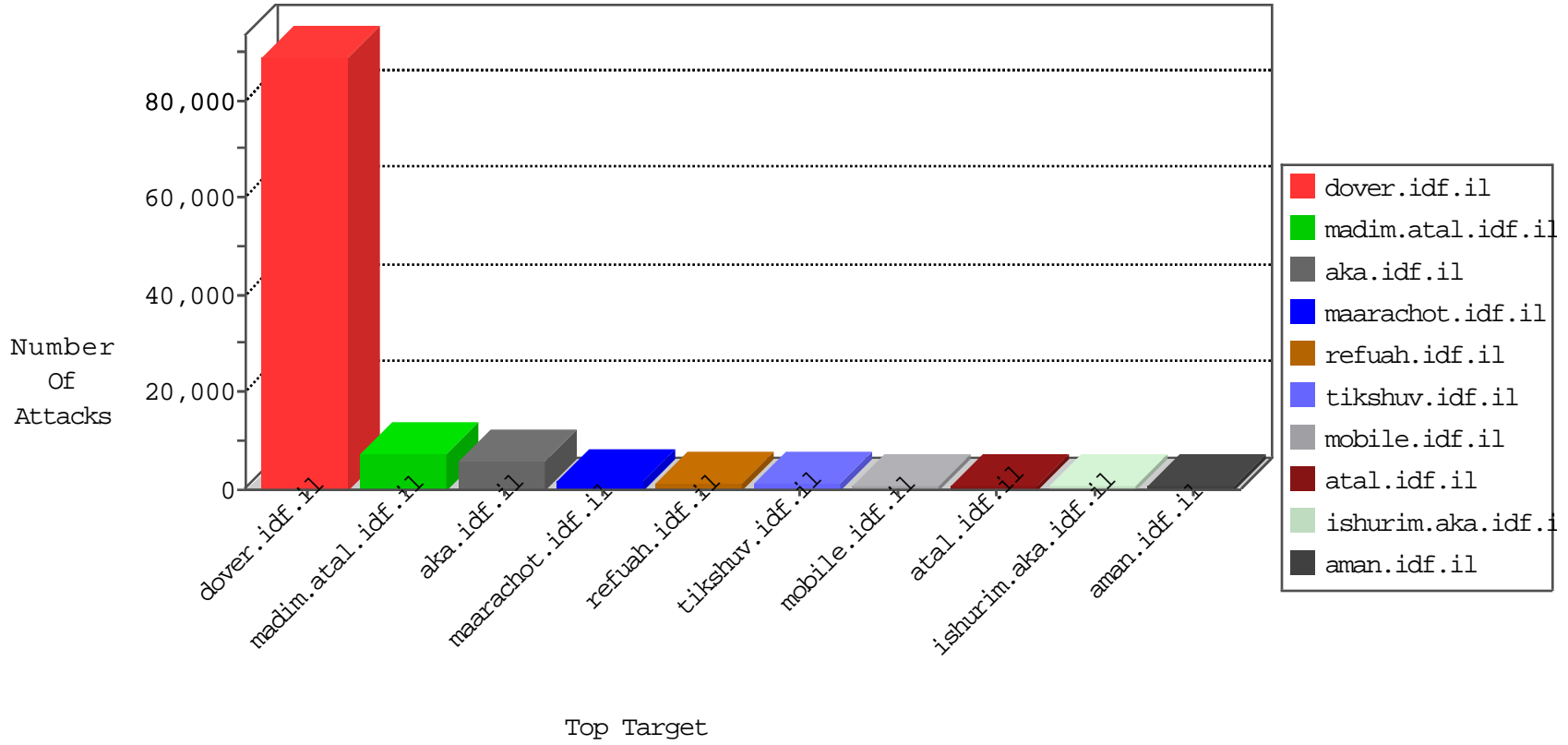


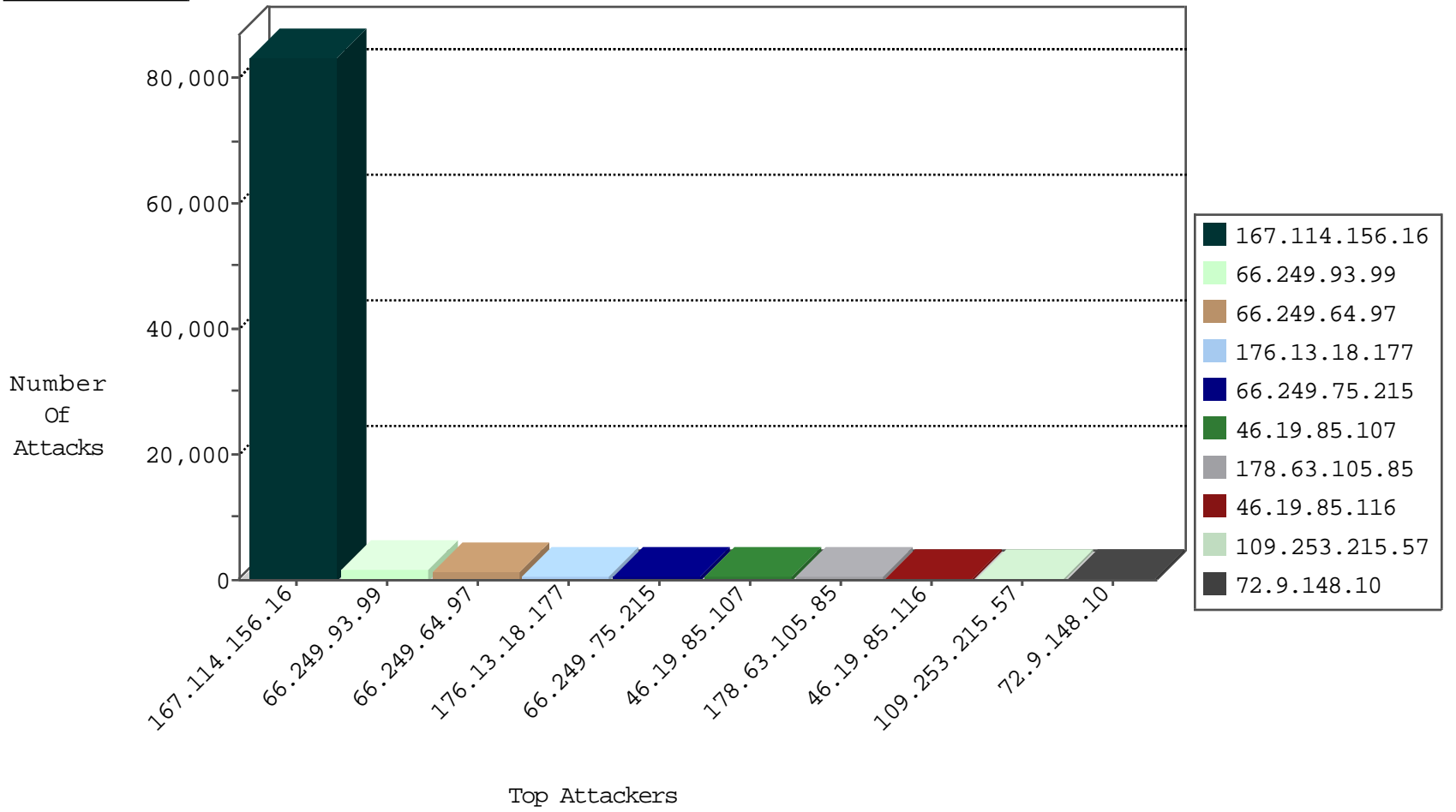
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	DOS-Tool-SwitchbladG	dest-reset	135103
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	508
176.13.14.144	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	463
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	99
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	57
46.19.85.42	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	33
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	24
46.19.86.246	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
5.22.129.78	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
62.0.102.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
79.181.33.5	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
2.54.7.59	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
79.183.231.16	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	9
2.52.177.52	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
94.230.84.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
46.19.86.79	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
85.64.249.42	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
82.145.218.194	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
46.19.86.35	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
109.160.172.43	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
79.182.38.184	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	6
84.111.81.211	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.65.112.218	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.182.38.184	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
91.227.71.250	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.54.147.162	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
213.57.91.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
185.130.5.193		147.237.76.30	himush.idf.il	Invalid TCP Flags	drop	5
192.117.9.90	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.253.195.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
185.130.5.193		147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	5
80.246.136.21	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.86.170	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
80.246.137.161	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.178.141.88	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.54.5.109	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
87.69.188.50	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.231.42	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
109.253.210.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
84.111.196.22	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.181.134.55	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.145.222.170	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
185.5.221.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.165.186	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
60.247.107.108	China	147.237.8.50	e.tikshuv.idf.il	I4 Source or Dest Port Zero	drop	3
168.235.197.20	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
84.111.169.143	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3

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	42
192.115.67.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	33
79.181.71.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	31
93.173.1.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	23
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
79.183.192.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
31.168.232.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
91.231.193.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
173.254.198.237	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
138.134.102.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
84.108.204.4	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
109.253.206.169	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
5.29.7.66	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
46.121.82.80	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
184.106.114.136	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
109.67.97.95	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.118.230	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
184.106.114.136	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
79.182.246.169	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.176.144.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.177.235.118	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
199.203.64.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
82.80.193.240	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
217.132.114.35	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.46.38.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.181.209.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.109.13.58	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.8.204.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
217.70.44.165	Sweden	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
80.178.67.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
89.203.221.120	Czech Republic	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	7
79.178.64.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.85.66	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.108.31.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.108.78.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
149.88.188.253	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.111.82.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
82.166.75.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
136.243.5.87	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	5
85.158.138.19	Germany	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
63.143.34.37	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
87.242.112.35	Russian Federation	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
202.124.109.87	New Zealand	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
94.102.153.58	United Kingdom	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
89.163.148.58	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
79.182.38.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
216.249.107.200	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
85.250.101.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.99	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1514
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1382
66.249.75.215	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	448
66.249.66.33	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	101
188.120.148.133	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	89
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	62
63.143.34.37	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	25
94.102.153.58	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	24
217.70.44.165	147.237.77.176	Sweden	matpash.idf.il	SQL Injection - Select From	17
178.63.18.196	147.237.76.86	Germany	navy.idf.il	SQL Injection - Select From	13
200.59.205.238	147.237.77.74	Argentina	law.idf.il	SQL Injection - Select From	12
216.185.43.135	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	12
213.8.145.99	147.237.77.233	Israel	atal.idf.il	SQL Injection - Select From	12
193.200.80.26	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	12
184.106.114.136	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
184.106.114.136	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	10
64.251.25.176	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
74.63.228.226	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	7
184.168.193.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
202.124.109.87	147.237.76.86	New Zealand	navy.idf.il	SQL Injection - Select From	6
23.91.70.119	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
64.31.44.6	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	6
184.173.233.226	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	6
70.89.127.78	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	6
156.184.49.210	147.237.77.216		dover.idf.il	ET SCAN NMAP -sA (2)	5
66.249.64.92	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
202.124.109.87	147.237.77.233	New Zealand	atal.idf.il	SQL Injection - Select From	4
87.242.112.35	147.237.76.31	Russian Federation	nakchal.idf.il	SQL Injection - Select From	4
97.88.198.223	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
195.234.228.90	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	3
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
216.249.107.200	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	3
66.249.69.137	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	2
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.69.93	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
46.19.85.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
46.116.134.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
104.238.98.124	147.237.72.166		aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.64.102	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
161.202.66.90	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	2
218.246.0.97	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	2
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
80.246.130.144	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
218.81.20.83	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
79.180.150.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
79.179.27.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18410
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1698
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	756
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	442
109.186.21.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	242
173.68.118.195	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	204
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	189
216.177.129.228	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	163
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
79.182.244.122	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	152
176.13.18.177	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	136
80.178.67.248	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	109
85.64.223.46	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
79.181.218.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	92
87.71.124.161	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
109.67.152.165	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
5.28.169.155	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
79.181.173.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
2.52.178.111	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	70
176.13.18.177	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	68
79.182.124.209	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	68
107.167.99.253	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	68
85.130.252.100	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
62.90.147.171	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	57
176.13.6.59	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	53
176.13.6.59	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	52
178.63.105.85	Germany	147.237.76.177	noore.idf.il	drop	SAM rule	drop	50
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	50
176.13.3.5	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
93.157.87.13	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	47
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	46
176.13.1.80	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	46
2.54.163.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
149.88.151.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
109.253.143.11	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	41
2.52.6.61	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	40
109.253.143.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
109.253.157.221	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.180.201.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.65.98.73	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
188.120.154.47	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
178.63.105.85	Germany	147.237.76.176	test.noore.idf.il	drop	SAM rule	drop	35
5.22.135.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
109.65.91.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
176.13.10.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
46.19.85.248	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	385
109.253.215.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	327
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	319
176.13.18.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	279
176.13.19.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	248
176.13.1.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	227
2.52.179.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	206
176.13.16.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	193
37.26.146.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	190
2.54.163.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	178
37.26.147.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	174
176.13.11.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	163
176.13.1.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
176.13.6.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	154
176.13.4.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
2.54.169.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	146
185.32.179.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
79.178.179.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
2.54.4.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	125
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
37.26.149.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
80.246.136.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
37.26.147.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
2.54.44.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
87.68.73.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
2.54.145.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
176.13.5.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
2.54.14.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
87.70.6.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
46.19.86.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
2.54.178.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
89.139.131.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
109.253.136.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
2.54.60.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
176.13.22.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
109.253.157.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
79.183.173.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.54.151.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
109.65.135.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
2.54.137.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
109.253.206.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
176.13.14.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
93.173.142.169	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	32