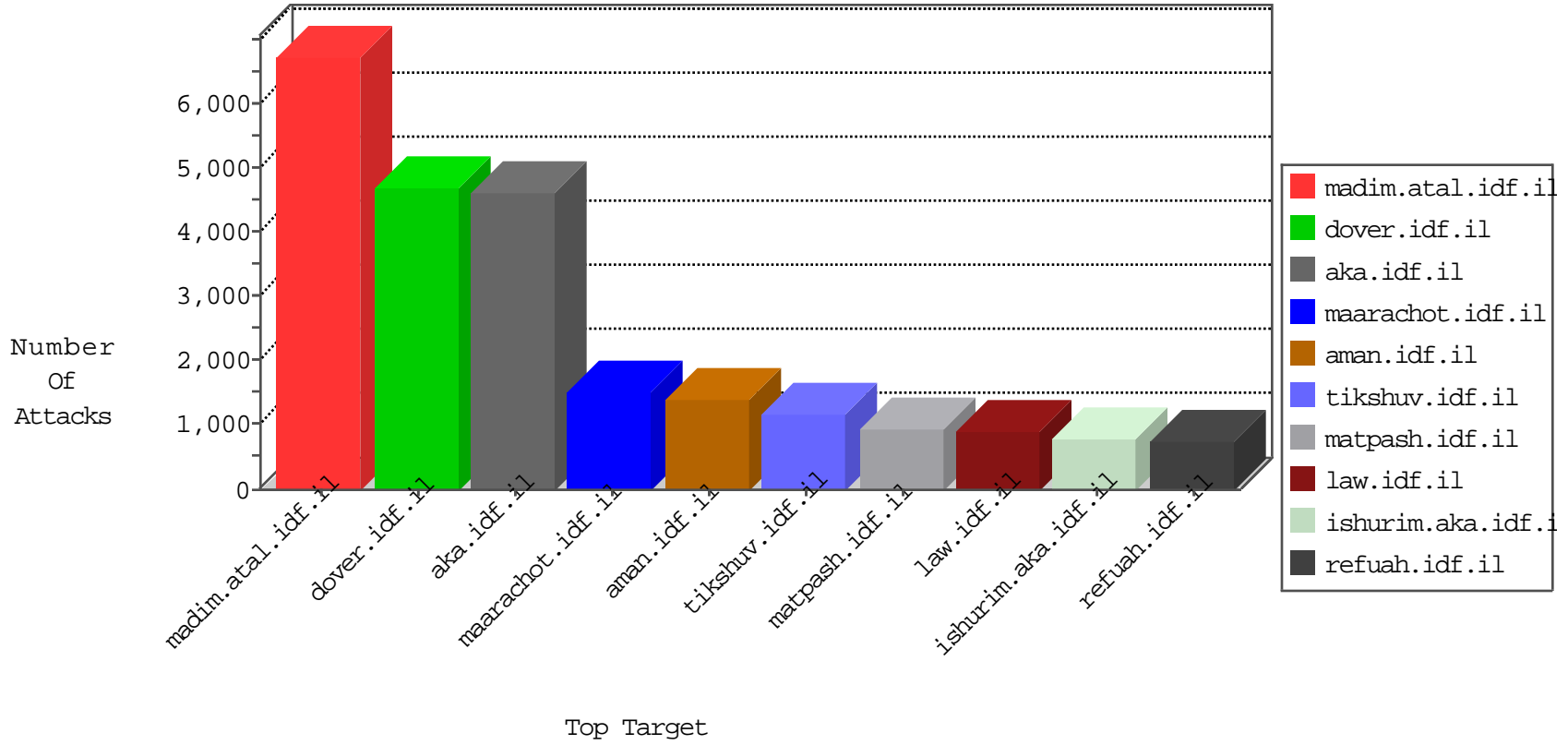


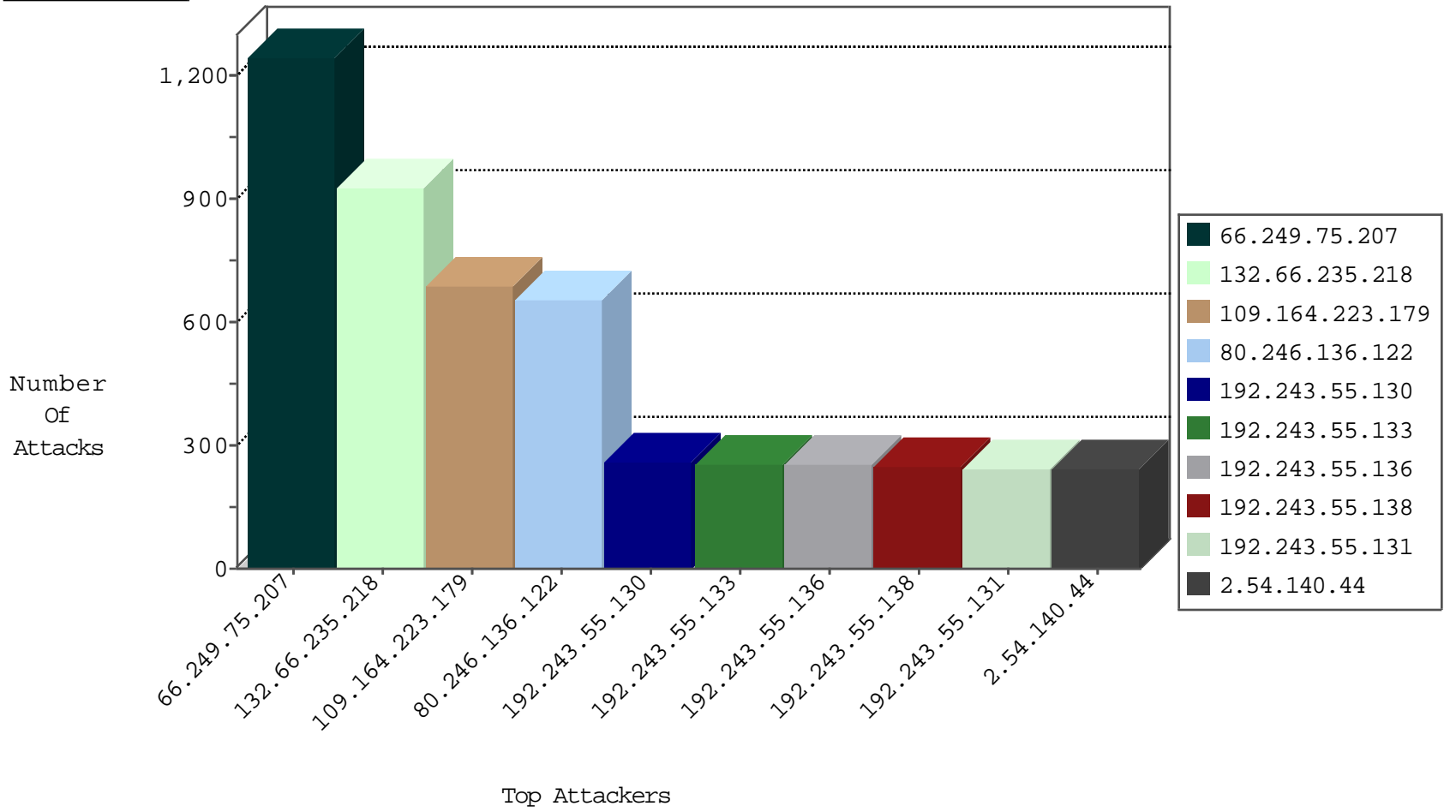
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.235.8.225	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3191
46.19.85.33	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	930
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	413
109.65.163.230	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	411
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	333
213.57.162.208	Israel	147.237.0.34	tikshuv.idf.il	HTTP-POST-Segmented-DoS	dest-reset	262
79.181.108.192	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	162
109.64.155.166	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	125
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
54.72.182.187	Ireland	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	85
80.246.139.53	Israel	147.237.77.216	doover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
81.218.65.210	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	62
82.145.208.48	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	58
82.145.222.228	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	45
84.111.125.88	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	33
82.145.222.87	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	20
109.64.224.141	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	20
0.0.0.0		147.237.77.216	doover.idf.il	HTTP Page Flood Attack	forward	18
109.64.28.234	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	17
82.145.209.166	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	15
2.52.33.192	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	15
82.145.219.34	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
194.90.128.185	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	15
82.145.217.30	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
114.79.13.54	Indonesia	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	10
114.79.45.202	Indonesia	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	9
82.145.209.28	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	7
87.69.114.68	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	6
82.145.222.189	Europe	147.237.77.216	doover.idf.il	Block_Ip_Web_In	drop	5
176.13.11.21	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.77.216	doover.idf.il	HTTP Page Flood Attack	drop	4
93.174.93.218	Netherlands	147.237.77.74	law.idf.il	block-sp-trafl	forward	4
81.218.171.201	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
46.19.85.63	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	3
81.218.8.34	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
136.243.48.85	Germany	147.237.77.216	doover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.8.34	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	3
109.253.216.224	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
136.243.48.82	Germany	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.179.173.189	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	3
87.69.165.171	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	3
81.218.8.34	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
136.243.48.82	Germany	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Http	drop	2
93.174.93.218	Netherlands	147.237.77.170	maarachot.idf.il	block-sp-trafl	forward	2
115.239.228.10	China	147.237.0.35	akaws.idf.il	JLM_Under_Attack_Con_Http	drop	2
80.74.102.34	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	2
46.19.85.173	Israel	147.237.77.216	doover.idf.il	SYN Flood out of context	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	30
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	29
85.64.4.23	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	27
79.177.242.24	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	24
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
123.126.113.163	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	21
89.139.147.111	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
109.64.141.99	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
79.181.134.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
61.135.189.69	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	13
79.182.148.237	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
81.218.251.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
62.219.12.85	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
98.126.130.202	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
82.166.115.233	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
85.65.93.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.178.102.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
84.108.77.11	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.26.149.226	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.70.75.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.64.243.213	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.131.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.71.65.111	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.78.120.205	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.142.118.83	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.8.241.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.179.199.166	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
147.235.236.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
66.76.174.2	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
66.249.93.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
37.26.146.186	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.183.60.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.179.60.195	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
212.29.223.233	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.65.143.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
37.26.149.197	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.85.51	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
109.253.202.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
79.183.179.152	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
217.70.44.165	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
176.13.1.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.76.174.2	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
178.203.146.227	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.75.207	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1244
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	67
66.76.174.2	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	24
67.228.38.74	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	12
66.76.174.2	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	12
216.185.43.135	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
217.70.44.165	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	6
185.32.179.225	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
84.245.33.104	147.237.77.176	Netherlands	matpash.idf.il	SQL Injection - Select From	6
185.32.179.128	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
212.179.132.202	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.75.231	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
209.126.116.147	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
81.218.190.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
209.126.116.147	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
79.182.141.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
108.163.253.194	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	2
106.57.58.197	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
31.7.185.23	147.237.76.39	Germany	mobile.meitav.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
37.26.146.151	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
37.26.149.209	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
83.143.81.94	147.237.77.74	Norway	law.idf.il	SQL Injection - Select From	2
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	2
46.116.25.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.21.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
106.57.58.197	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
85.250.210.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.2.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.117.59.18	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.148.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.241.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.73.74.224	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.113	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.6.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.163.253.194	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sA (2)	1
93.174.93.181	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
199.203.196.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.164.223.179	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	683
132.66.235.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	363
132.66.235.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	360
79.182.28.130	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	204
132.66.235.218	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	150
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	148
37.26.149.238	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
2.53.16.191	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	129
149.88.230.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	120
37.46.38.173	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	111
87.71.27.6	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
188.120.154.11	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
31.171.244.115	Switzerland	147.237.77.216	dover.idf.il	drop	SAM rule	drop	93
109.253.135.52	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	79
85.130.239.134	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
175.157.206.9	Sri Lanka	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	69
31.171.244.115	Switzerland	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	62
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	61
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	49
109.65.59.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
87.70.26.203	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	48
84.228.166.53	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
136.243.48.85	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	42
176.13.14.127	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
80.246.137.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	36
79.182.16.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
79.176.54.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
46.19.85.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
132.64.27.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	32
36.80.111.124	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
176.13.19.191	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	32
175.157.206.9	Sri Lanka	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
2.52.133.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.131	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	30
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
185.24.207.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	28
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	651
109.186.24.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	230
185.32.179.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	201
79.181.218.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	193
2.54.134.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	193
176.13.2.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	188
109.253.216.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	182
176.13.11.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	177
2.54.32.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	156
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	149
37.26.146.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
46.19.86.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
185.32.179.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
2.54.191.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
2.54.152.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
109.253.143.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
176.13.14.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
109.65.35.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
176.13.7.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
83.136.253.188	United Kingdom	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 83.136.253.188	Block	109
2.54.41.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.85.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
37.26.146.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
37.26.149.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
81.218.156.79	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	91
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
2.54.3.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
176.13.2.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
46.19.85.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
109.253.214.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
176.13.12.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
109.253.221.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
2.54.15.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
80.246.136.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
37.26.147.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
176.13.6.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
37.26.149.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
37.26.146.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	47
109.253.133.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
80.246.137.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
185.32.179.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
109.253.203.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
176.13.21.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
109.253.192.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38