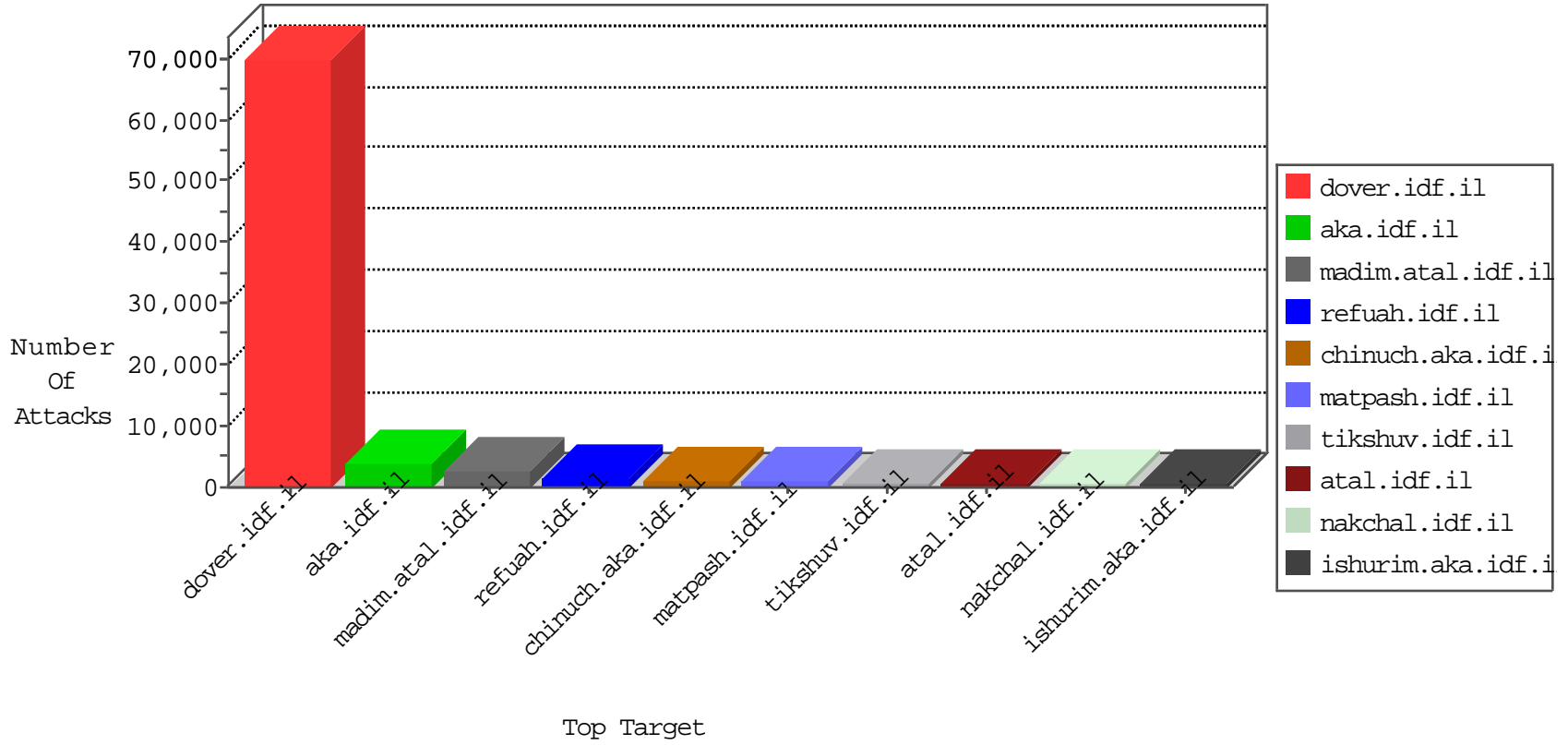


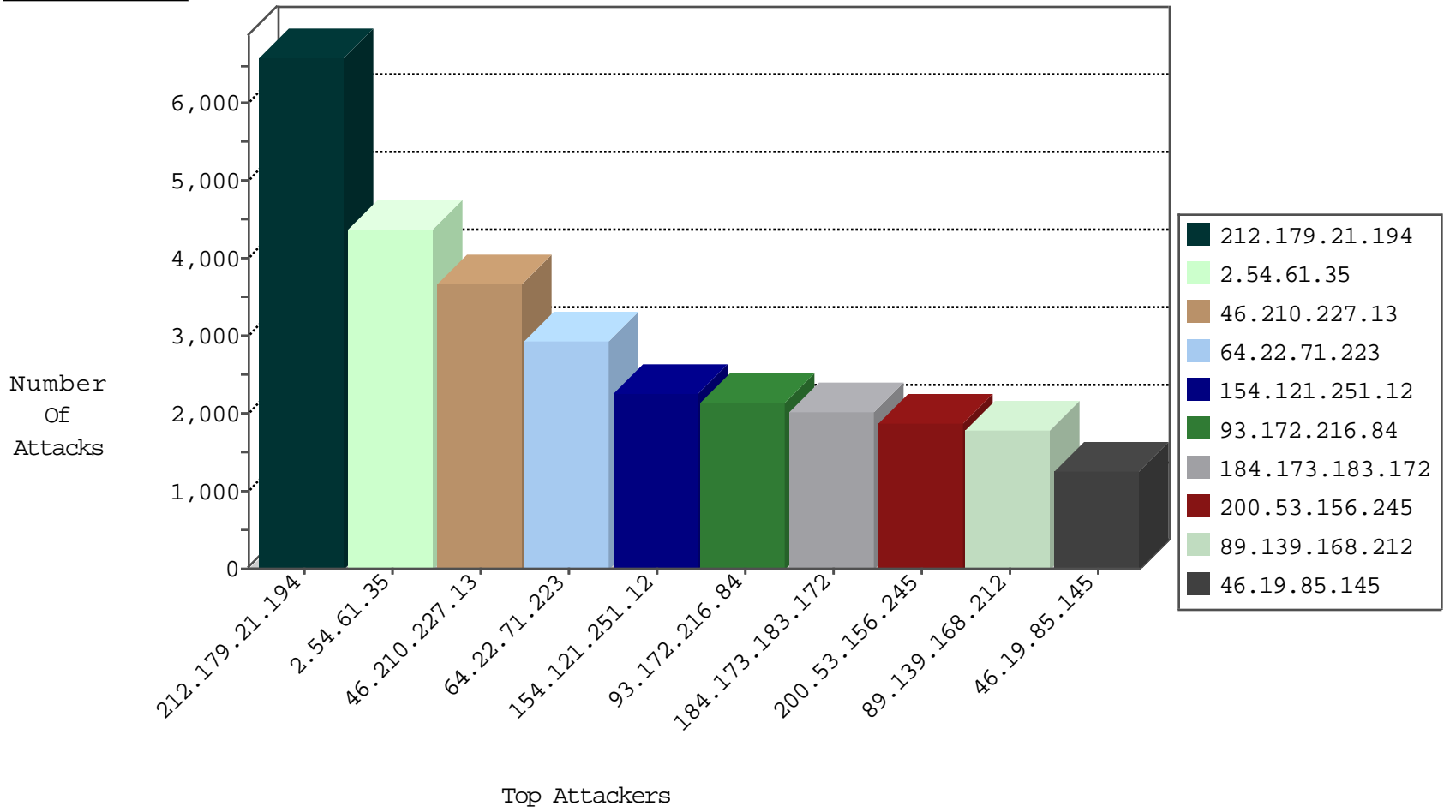
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
212.117.143.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5797
81.218.126.226	Israel	147.237.76.86	navy.idf.il	TCP Scan (vertical)	drop	3743
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2869
79.177.184.191	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2578
220.181.108.94	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	1170
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	904
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	644
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	567
81.218.126.226	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	509
220.181.108.177	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	501
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	477
109.64.204.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	380
154.121.251.12		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	375
79.177.118.34	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	367
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	279
77.125.138.128	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	262
37.26.148.207	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	250
81.218.200.154	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	235
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	234
79.179.167.41	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
220.181.108.107	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	216
220.181.108.183	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	203
220.181.108.97	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	199
37.142.187.24	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
84.228.163.233	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
85.64.115.193	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
79.179.185.1	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
79.177.224.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
220.181.108.104	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	155
109.160.234.221	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
46.19.86.86	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	146
109.64.126.122	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
212.235.43.208	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
84.94.59.18	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
220.181.108.80	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	122
79.178.184.248	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
84.229.28.44	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
84.228.33.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
212.143.119.98	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
2.54.37.29	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
212.199.218.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
192.116.142.138	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
84.229.166.120	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
2.54.168.189	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
89.138.79.163	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
220.181.108.83	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	78
46.121.248.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
5.29.117.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.94.45.223	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1147
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	685
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	532
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	348
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	272
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	144
184.173.183.172	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_P-N_40-59	Permit	140
77.125.87.161	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	113
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	45
212.199.251.227	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	33
89.139.168.212	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	24
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	21
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
96.47.226.21	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	19
212.25.102.63	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
89.138.248.247	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
116.251.221.203	Singapore	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	7
212.199.97.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
87.68.68.200	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.29.202.206	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
80.246.136.82	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.180.219.157	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.150.174.180	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
192.114.91.215	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.182.127.196	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.178	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.210	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	5
84.229.248.78	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
122.107.249.146	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.208	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
85.64.228.45	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
83.130.100.227	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
79.179.191.120	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	196
80.247.229.174	France	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	47
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
199.203.59.121	Israel	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
81.218.77.162	Israel	147.237.77.74	law.idf.il	GPL SCAN nmap TCP	3
46.210.227.13	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
200.53.156.245	Mexico	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
37.142.64.179	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.19.86.223	Israel	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.136.152	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
192.3.108.133	United States	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
37.142.249.29	Israel	147.237.76.31	nakchal.idf.il	OS-WINDOWS Microsoft Windows WebDAV propfind access	2
37.60.45.81	Israel	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
149.78.154.69	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.131	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
176.12.150.16	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
109.237.26.139	United Kingdom	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
180.169.22.21	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
52.28.93.27	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
118.97.20.66	Indonesia	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
5.199.172.36	Lithuania	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
94.230.86.144	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.139	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	Cote D'Ivoire	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
61.160.224.130	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
141.212.122.122	United States	147.237.72.156	anan.idf.il	ET SCAN Potential SSH Scan	1
43.255.188.131	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
109.64.169.22	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
2.54.35.190	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
91.22.4.193	Germany	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
221.235.189.245	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
192.3.108.133	United States	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
59.160.110.163	India	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
123.196.126.107	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.188.130	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.207.136.109		147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.0.119	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.183.128.6	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
162.248.143.132	Canada	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6449
2.54.61.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4396
46.210.227.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3650
93.172.216.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2153
154.121.251.12		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1956
89.139.168.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1713
200.53.156.245	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1708
46.19.85.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1249
82.145.222.111	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1209
95.86.116.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1024
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	851
82.145.222.16	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	816
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	616
164.138.119.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	554
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	518
46.116.158.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	511
109.186.18.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	498
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	436
81.218.126.226	Israel	147.237.76.42	refuah.idf.il	number of HTTP headers exceeded allowed maximum of 500	HTTP Format Sizes	monitor	427
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	424
212.143.119.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	417
64.22.71.223	United States	147.237.76.147	chinuch.aka.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	405
199.190.46.103	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	352
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	315
2.54.188.36	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	314
82.132.213.98	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	313
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	260
198.8.80.223	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	258
2.54.132.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	254
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	251
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	238
84.94.32.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
46.19.85.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	228
93.173.182.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	222
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	220
93.173.152.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	218
50.118.162.167	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	218
70.25.122.234	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	211
79.176.194.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	202
64.22.71.223	United States	147.237.0.34	tikshuv.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	202
95.86.97.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	187
93.172.38.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	176
37.238.164.4	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	175
84.108.148.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	174
203.116.187.1	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	172
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	170
66.171.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	155
64.22.71.223	United States	147.237.76.31	nakchal.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	148
64.22.71.223	United States	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	138

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
64.22.71.223	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	701
79.183.35.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	687
64.22.71.223	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	375
87.68.35.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	276
64.22.71.223	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	270
176.12.150.16	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.150.16	Block	231
154.121.251.12		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 154.121.251.12	Block	206
5.29.70.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
80.246.136.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	184
81.218.200.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	182
81.218.200.154	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.200.154	Block	142
46.116.244.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	136
64.22.71.223	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	133
2.54.176.132	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.176.132	Block	94
176.12.137.134	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.134	Block	87
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	83
197.193.24.166	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	80
109.253.145.5	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.145.5	Block	62
37.26.146.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
64.22.71.223	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	58
80.247.229.174	France	147.237.72.166	aka.idf.il	PHP Attempt	Block	47
2.54.37.122	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.37.122	Block	44
64.22.71.223	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	42
64.22.71.223	United States	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	41
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	37
109.64.30.60	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.30.60	Block	36
109.253.137.101	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.137.101	Block	34
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	26
80.247.229.174	France	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 80.247.229.174	Block	23
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	21
64.22.71.223	United States	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning	Block	20
2.54.137.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.137.214	Block	20
79.177.171.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	18
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	15
79.177.183.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	14
31.210.191.197	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.210.191.197	Block	12
64.22.71.223	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	12
84.108.46.29	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	11
31.168.82.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
77.127.223.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
213.151.59.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
64.22.71.223	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	10
212.179.21.194	Israel	147.237.77.74	law.idf.il	Suspicious Response Code	Block	9
37.26.148.232	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
80.178.168.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
185.32.178.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
46.120.178.26	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	8
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	7
82.80.52.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7