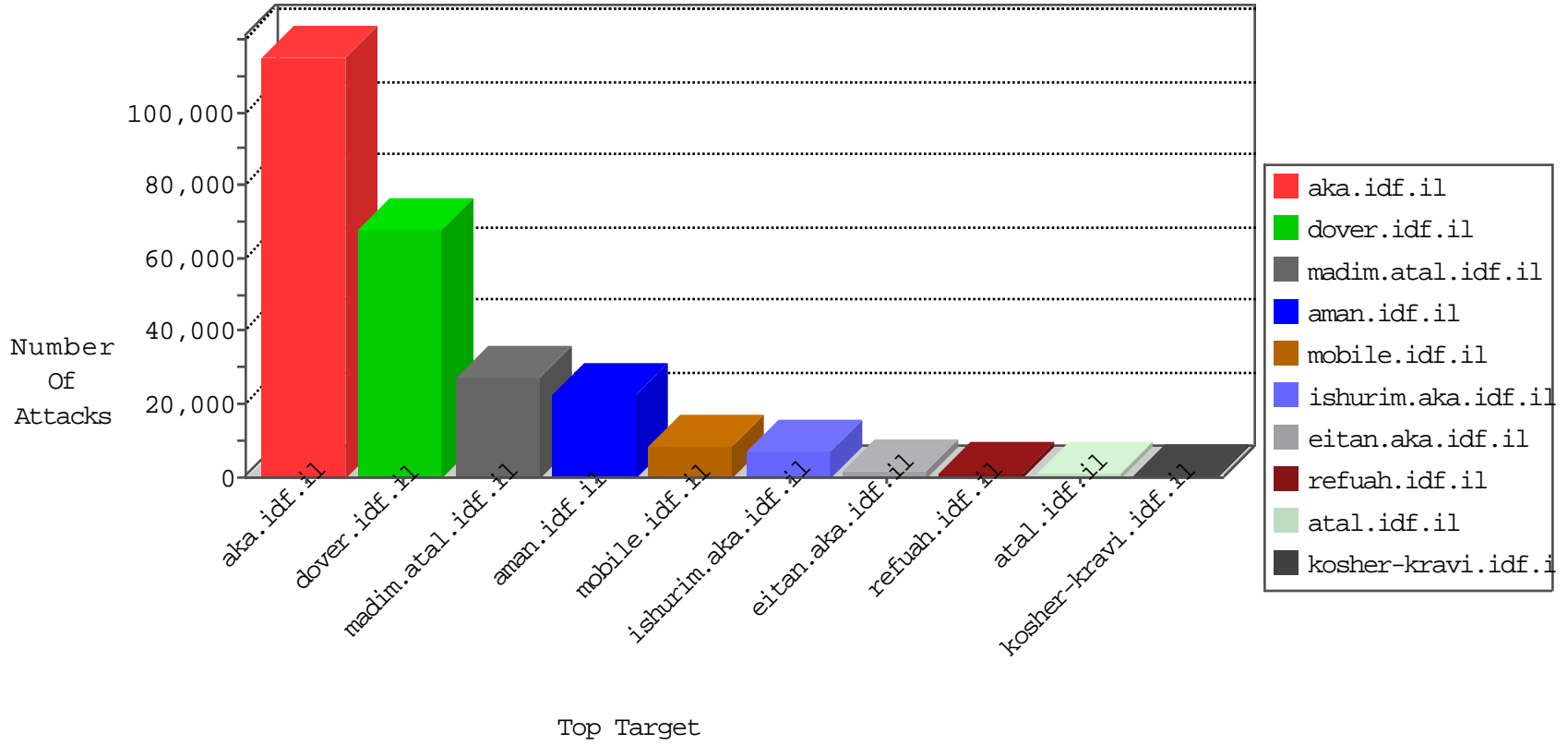


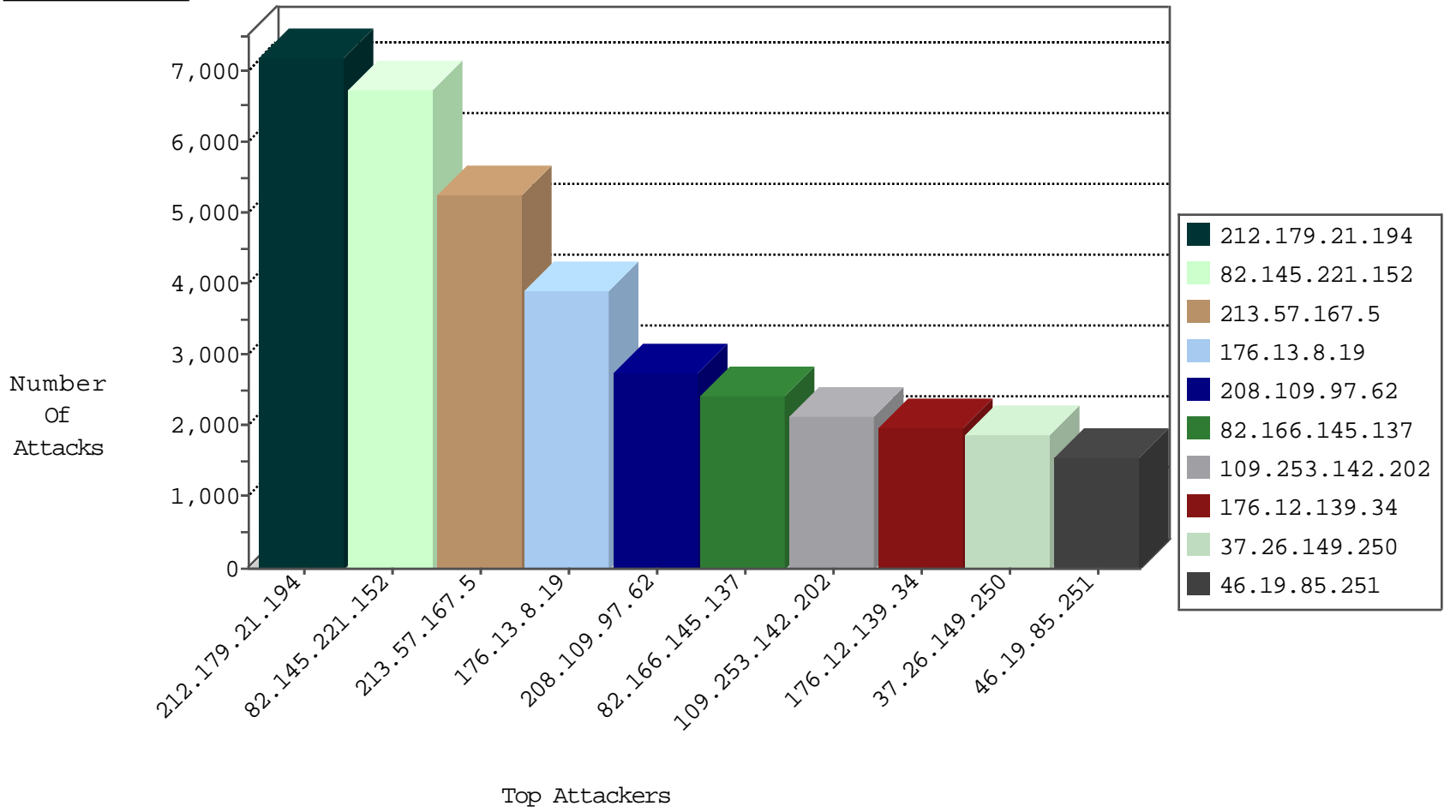
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.93.160	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3014
220.181.108.85	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	675
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	456
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	396
46.19.85.227	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	256
220.181.108.163	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	179
79.178.169.131	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	161
176.106.227.151	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	153
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
77.125.0.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	107
176.12.146.60	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	93
82.166.23.110	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	77
84.108.102.3	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	77
213.151.38.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	75
2.54.16.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	49
188.120.148.234	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	37
2.54.180.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	33
2.54.16.142	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	32
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	30
79.180.96.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
2.52.51.38	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
185.32.179.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
46.19.85.192	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
46.19.85.41	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
194.90.83.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
109.67.132.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	18
66.249.64.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	16
176.106.226.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
193.43.244.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
46.19.85.39	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
37.142.145.21	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
37.26.149.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
87.69.171.7	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
2.54.1.26	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
176.12.143.182	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
46.19.86.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
194.90.225.101	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
82.145.219.150	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
82.80.17.247	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
46.31.103.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
2.54.170.158	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
81.218.182.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
109.253.135.215	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
199.203.53.3	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
192.168.40.53		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
82.166.23.79	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
176.13.22.56	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
89.138.84.183	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.106.226.161	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	16
176.106.226.161	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	12
166.197.155.255	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	11
79.179.164.96	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	11
93.173.232.34	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
31.154.86.155	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
83.139.133.17	Russian Federation	147.237.77.216	dover.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	8
176.106.226.2	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
212.150.215.8	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
46.19.85.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	7
84.229.31.54	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
176.106.227.88	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
213.8.41.250	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
131.107.80.31	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
46.116.162.11	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
46.19.85.69	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
46.19.85.157	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
84.111.20.117	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
46.19.85.95	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
85.64.107.224	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
176.106.227.131	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
121.146.93.228	Korea, Republic of	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
79.180.210.68	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
80.178.136.94	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
46.121.97.32	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
31.168.25.215	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
109.66.182.167	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
109.64.155.209	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
46.19.85.84	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
149.88.80.227	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
176.106.227.7	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
79.178.49.165	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
62.90.255.56	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.26.149.234	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
176.106.226.210	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
109.65.102.224	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
87.69.40.139	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
77.127.179.80	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.140	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
37.26.149.249	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
79.181.172.126	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.227	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
85.250.185.164	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
109.65.164.174	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.210.235.116	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.28	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
209.206.230.67	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
79.178.169.243	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
2.54.6.128	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
2.54.140.248	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	114
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	70
104.207.147.244		147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	16
213.204.103.36	Lebanon	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	5
46.19.85.199	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
213.204.103.36	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	4
106.137.118.149	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	3
82.166.23.79	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.247	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.100	Netherlands	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
94.102.49.102	Netherlands	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
208.109.97.62	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
183.60.175.149	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 2048	2
37.142.68.25	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
106.137.118.149	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
208.68.36.51	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
183.60.175.149	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -f -sS	2
85.113.113.105	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
106.137.118.149	Japan	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
91.143.18.32	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
213.106.240.194	United Kingdom	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.100	Netherlands	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
91.143.18.32	Russian Federation	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.206	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
106.137.118.149	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
106.137.118.149	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.69.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
106.137.118.149	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
106.137.118.149	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.143	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
31.154.180.77	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
93.174.93.100	Netherlands	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
106.137.118.149	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
207.232.27.5	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
91.143.18.32	Russian Federation	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
128.199.140.140	Singapore	147.237.77.74	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
91.143.18.32	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
176.12.143.159	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
212.76.168.42	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
66.249.84.137	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
94.102.49.102	Netherlands	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
213.192.33.191	Czech Republic	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
212.76.168.42	Russian Federation	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
66.249.75.240	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.100	Netherlands	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.70	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
106.137.118.149	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2

## 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	6926
82.145.221.152	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6725
208.109.97.62	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	1693
46.19.85.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1567
192.114.23.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1388
212.25.102.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	943
208.109.97.62	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	895
94.252.170.155	Syrian Arab Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	861
87.68.31.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	812
82.145.223.148	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	709
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	708
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	700
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	677
13.21.125.9	United Kingdom	147.237.0.15	kosher-kravi.idf.il	First packet isn't SYN	drop	drop	468
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	468
2.52.30.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	463
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	461
192.115.177.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	459
132.66.22.36	Israel	147.237.76.200	eitan.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	453
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	437
37.228.105.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	412
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	408
165.189.255.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	401
13.21.125.9	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	365
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	363
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	359
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	352
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	345
212.243.165.114	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	315
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	313
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	282
104.240.22.111		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	272
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	267
91.133.217.127	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	266
91.133.217.127	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	266
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	265
66.87.129.242	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	251
206.132.225.54	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	245
176.18.68.150	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	232
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	231
37.26.149.208	Israel	147.237.76.200	eitan.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	228
167.91.0.225	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	221
2.54.57.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	218
2.54.184.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	218
13.21.125.9	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	212
194.157.243.82	Finland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	210
109.110.112.90	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	201
5.255.253.19	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	195
113.197.14.2	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	191
79.179.60.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	183

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.167.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5242
176.13.8.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3909
82.166.145.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2413
109.253.142.202	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.142.202	Block	2136
176.12.139.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1979
37.26.149.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1845
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.155	Block	1424
46.19.86.72	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.72	Block	1266
109.253.149.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1169
176.13.15.112	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.15.112	Block	1096
46.19.85.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1008
176.13.2.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	966
176.13.22.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	516
176.12.137.195	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.195	Block	492
176.13.17.56	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.17.56	Block	426
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	336
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	306
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	300
109.253.142.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	271
109.253.138.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	258
176.106.46.74	Palestinian Territory, Occupied	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 176.106.46.74	Block	246
149.78.135.42	United States	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/popups/markivsachar.aspx parameter	None	240
109.253.129.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	228
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	216
68.180.229.239	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	198
66.249.78.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	192
132.66.22.36	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 132.66.22.36	Block	186
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	180
176.12.139.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
66.249.67.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	162
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	156
66.249.93.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	156
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	150
66.249.93.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	150
66.249.78.141	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	144
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	138
46.120.100.171	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	132
66.249.67.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	132
66.249.67.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	132
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	132
66.249.78.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	132
66.249.78.134	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	132
66.249.78.148	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	132
84.228.33.225	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	132
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	120
66.249.78.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	114
66.249.93.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	114
157.55.39.191	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	108
85.250.68.24	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	102
91.144.82.226	Hungary	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/popups/markivsachar.aspx parameter	None	102