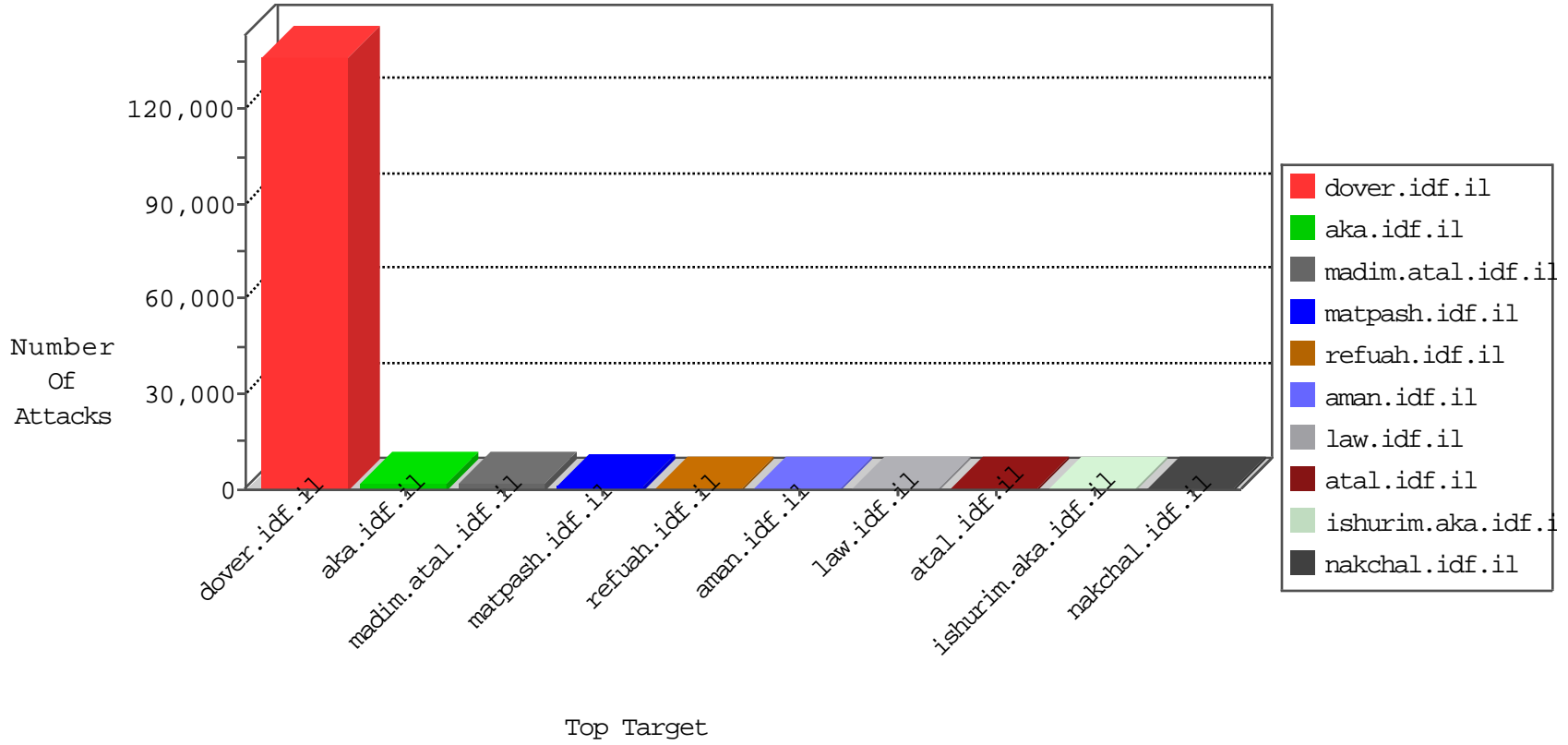


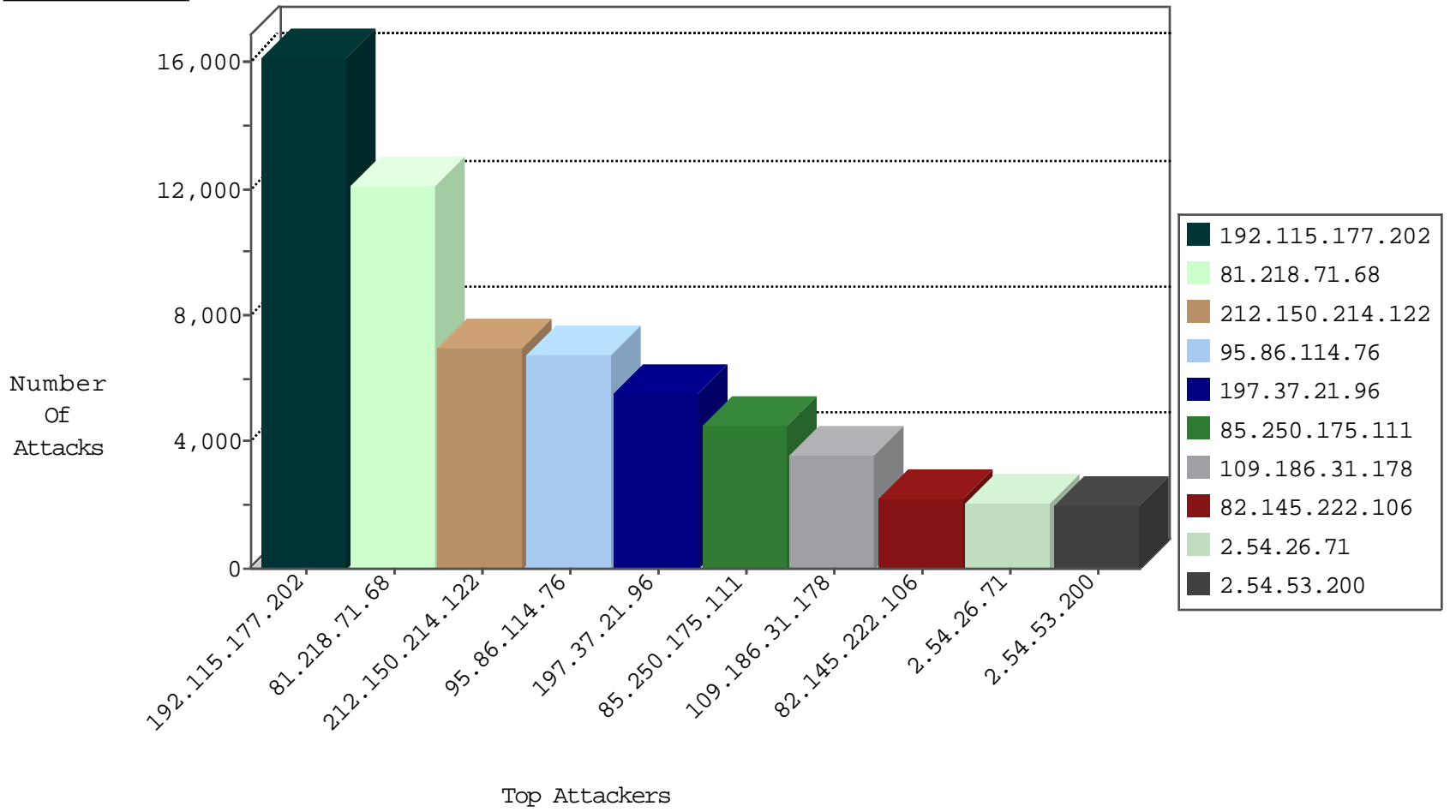
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
198.52.155.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	174961
46.19.86.242	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6082
200.53.156.138	Mexico	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3991
66.249.69.76	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3746
66.249.75.60	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3491
66.249.81.218	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3424
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2821
178.214.74.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2736
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2720
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2710
66.249.75.68	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2094
66.249.69.92	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1863
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1675
66.249.69.84	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1440
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	543
200.53.156.132	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	535
198.52.155.201	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	483
66.249.73.217	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	443
192.114.91.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	408
109.186.18.208	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	391
94.159.210.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	371
77.126.151.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	356
87.68.208.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	330
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	299
46.121.242.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	284
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	280
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	263
212.143.186.38	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	262
212.110.92.34	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	231
66.249.67.65	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	219
66.249.93.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	212
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	202
46.120.143.171	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	191
79.178.57.141	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	186
46.120.34.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	185
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
5.28.161.168	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
79.180.167.98	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
77.127.158.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
37.26.147.229	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
132.73.204.117	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
176.12.143.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
79.178.203.192	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	159
66.249.93.200	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	133
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
79.177.153.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	118

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	759
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	232
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	162
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	125
184.173.183.172	United States	147.237.76.200	eitan.aka.idf.il	DVRep_P-N_40-59	Permit	121
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	99
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	42
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	30
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	22
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	19
198.52.155.201	United States	147.237.77.216	dover.idf.il	C1000155: HTTP: OPTIONS methods	Permit	12
198.190.245.10	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
79.182.145.131	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	8
79.177.184.127	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	7
85.250.175.111	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
218.77.79.43	China	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	7
79.182.37.46	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
213.139.52.29	Jordan	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
218.77.79.43	China	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	6
77.126.229.159	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
218.77.79.43	China	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	5
54.64.39.80	United States	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	5
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	5

Top Attackers In ID

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	102
46.19.85.162	Israel	147.237.76.42	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
85.250.175.111	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	7
198.52.155.201	United States	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
66.249.75.68	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.69.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
109.253.131.133	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	3
43.255.188.135	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	3
61.183.128.6	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	3
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.134	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.131	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.132	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.69.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.151	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
43.255.188.135	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.147	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.134	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
213.57.21.82	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
61.183.128.6	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
58.213.123.107	China	147.237.76.39	mobile.meitav.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number	2
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
58.213.123.107	China	147.237.76.31	nakchal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number	2
80.246.136.207	Israel	147.237.72.156	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
43.255.188.131	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
196.47.173.21	Cote D'Ivoire	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.135	Japan	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
58.213.123.107	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
192.115.177.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16199
81.218.71.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12146
212.150.214.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7018
95.86.114.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6763
197.37.21.96	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5526
85.250.175.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4328
109.186.31.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3573
82.145.222.106	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2204
2.54.26.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2068
2.54.53.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2010
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1814
82.145.222.144	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1533
5.29.133.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1255
173.245.65.74	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1119
95.86.124.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	959
212.179.61.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	842
66.249.81.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	818
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	813
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	791
66.249.81.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	783
193.106.54.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	636
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	576
95.86.122.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	551
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	550
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	528
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	526
200.53.156.132	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	508
46.253.95.186	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	472
109.186.0.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	458
109.47.2.229	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	439
165.50.243.168		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	418
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	413
199.101.204.250	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	412
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	405
66.102.8.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	405
66.102.8.178	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	404
66.249.83.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	404
2.54.161.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	404
66.249.83.158	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	397
66.102.8.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	393
66.249.83.155	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	390
62.207.60.229	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	373
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	348
109.186.18.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	345
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	336
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	335
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	328
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	322
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	304
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	303

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.140.133	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.140.133	Block	427
84.228.1.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	265
176.12.145.66	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.145.66	Block	165
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	164
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	153
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	135
109.253.131.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	118
109.253.140.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	109
87.69.77.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90
176.13.17.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	85
2.52.11.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
192.116.172.33	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 192.116.172.33	Block	75
176.12.148.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	47
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
173.208.235.162	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	41
79.183.220.15	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	35
173.208.235.162	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 173.208.235.162	Block	33
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	29
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	25
2.54.10.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
46.19.85.160	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.160	Block	23
2.52.42.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
109.253.142.141	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.142.141	Block	20
200.53.156.132	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	18
176.12.150.15	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.150.15	Block	16
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	15
173.208.235.162	United States	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 173.208.235.162	Block	14
176.8.91.130	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15081-he/	Block	10
84.111.138.28	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	9
79.183.220.15	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	9
109.226.15.199	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	9
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	8
109.66.106.230	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/resource/userfollowresource/create/	Block	8
157.55.39.63	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
79.182.174.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
41.218.189.149	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	7
192.99.3.171	Canada	147.237.77.74	law.idf.il	PHP Attempt	Block	6
157.55.39.195	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
85.250.255.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	6
200.53.156.138	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
99.122.109.223	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
41.129.67.85	Egypt	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	6
212.76.108.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
37.115.189.89	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15081-he/	Block	6
82.166.146.20	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	5
109.226.15.199	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
207.46.13.115	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
109.226.15.199	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	5