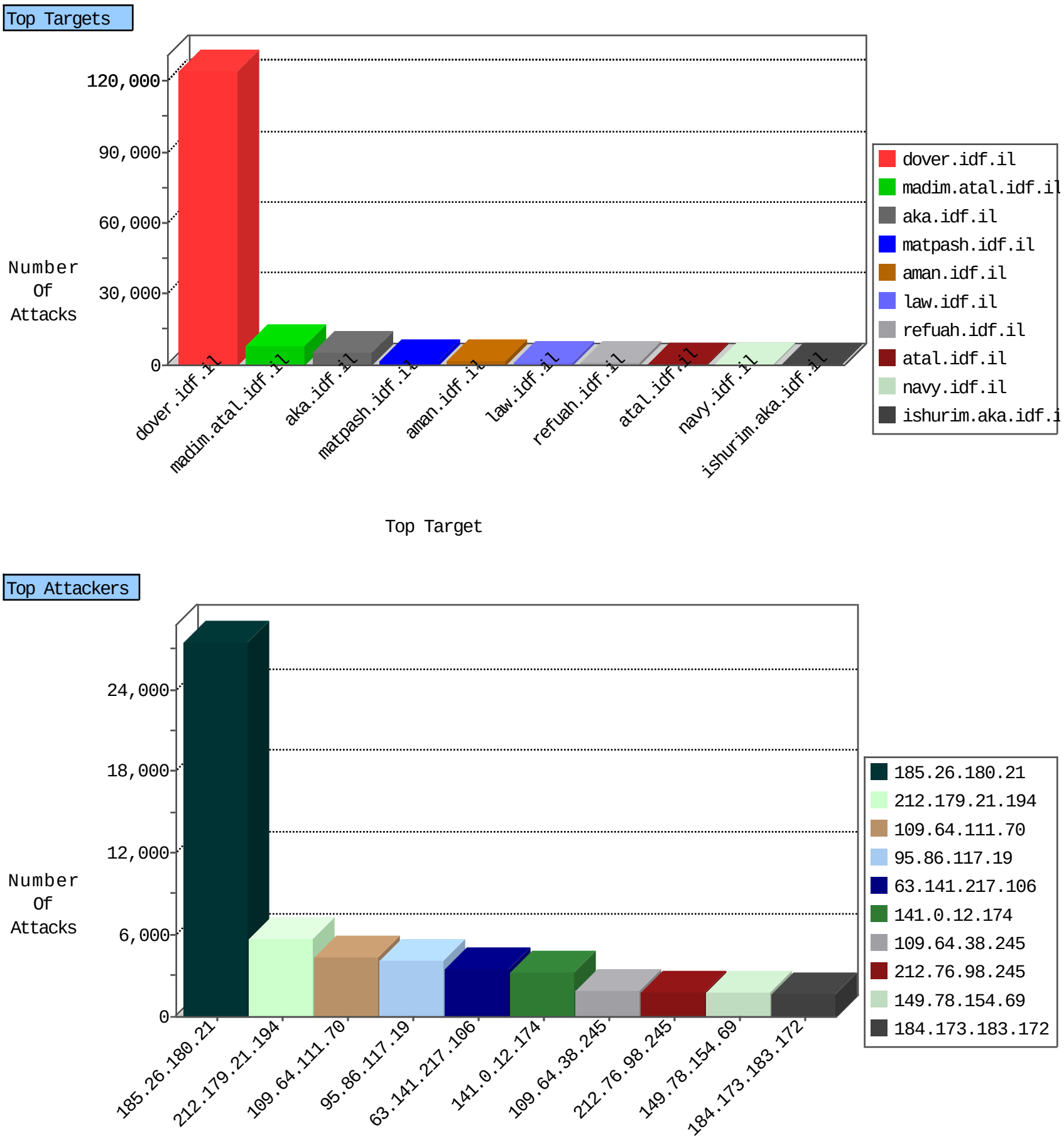
06-17-2015-00:00:04 to 06-18-2015-00:00:04

IDF Under Attack Daily Report



06-17-2015-00:00:04 to 06-18-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
185.26.180.21	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6719
66.249.65.5	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2351
213.8.71.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	751
63.141.217.106	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	675
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	581
84.109.154.171	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	567
79.179.102.135	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	464
66.249.73.185	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	448
37.142.138.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	399
176.65.17.163	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	355
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	329
5.29.219.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	319
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	318
80.246.136.223	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	312
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	306
66.249.73.211	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	256
15.195.185.82	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	242
93.173.139.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
80.230.101.180	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	226
87.69.181.222	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	223
192.114.2.36	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	219
195.95.183.254	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
149.88.91.210	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	180
84.228.11.238	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
74.101.93.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	156
213.8.71.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	155
5.29.117.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	147
212.76.118.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	144
198.208.240.250	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	141
168.235.198.150		147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	134
46.116.186.215	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
79.176.62.14	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
109.64.164.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	122
213.57.183.105	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	117
5.102.254.205	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	112
79.181.57.8	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
77.125.160.185	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
66.249.64.151	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	96
46.19.86.122	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
46.19.86.213	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
176.12.150.82	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
185.32.178.132	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
46.19.86.93	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
84.111.80.237	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	85
84.95.199.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
37.142.0.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81

06-17-2015-00:00:04 to 06-18-2015-00:00:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.111.70	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	3242
109.64.111.70	Israel	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	1185
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	699
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	470
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	330
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	226
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	169
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	142
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	30
194.114.146.227	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
178.234.102.95	Russian Federation	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
31.168.96.254	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
37.26.146.233	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
46.19.86.241	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
66.240.192.138	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	7
79.182.129.44	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	6
87.68.25.141	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	6
213.139.52.16	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	6
176.228.178.161	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
109.64.136.243	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
166.184.167.244	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	5
82.80.170.35	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	5
79.183.19.38	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4

06-17-2015-00:00:04 to 06-18-2015-00:00:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.65.48	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	363
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	37
180.92.196.86	Australia	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	8
41.238.32.104	Egypt	147.237.77.216	dover.idf.il	SQL Injection - Select From	7
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	4
149.88.112.48	United States	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	4
91.109.14.128	United Kingdom	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	3
61.183.128.6	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.133	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
195.244.23.42	Israel	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.134	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
109.253.157.154	Israel	147.237.72.166	aka.idf.il	GPL SCAN myscan	2
43.255.188.135	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
104.243.24.211		147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
199.203.59.121	Israel	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
1.254.6.66	Korea, Republic of	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
95.86.64.238	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
128.199.207.123	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
43.255.188.134	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
50.176.154.241	United States	147.237.76.42	refuah.idf.il	Tehila - Perl LWP with fake user agent	2
43.255.188.135	Japan	147.237.8.27	e.madim.atal.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
43.255.188.133	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.158	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
109.253.157.154	Israel	147.237.72.166	aka.idf.il	INDICATOR-SCAN myscan	2
66.249.73.225	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
43.255.188.135	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.60	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
199.203.59.121	Israel	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.45	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.133	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
89.188.101.10	Russian Federation	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
212.150.174.66	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.125.4	Turkey	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
62.212.73.138	Netherlands	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
190.90.13.17	Colombia	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.188.135	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
101.187.109.172	Australia	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1

06-17-2015-00:00:04 to 06-18-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.26.180.21	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27520
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5576
95.86.117.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4100
63.141.217.106	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3539
141.0.12.174	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3216
109.64.38.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1886
212.76.98.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1815
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1755
2.54.133.153	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1629
212.76.96.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1564
46.19.85.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1474
212.179.159.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	856
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	816
8.37.224.86	Anonymous Proxy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	779
85.250.140.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	777
212.199.227.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	732
15.195.185.82	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	708
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	638
31.168.169.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	613
212.76.116.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	592
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	554
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	521
203.241.152.103	Korea, Republic of	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	512
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	462
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	461
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	457
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	444
172.16.255.105		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	440
85.250.214.33	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	415
66.249.84.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	391
66.249.84.188	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	378
66.249.84.182	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	377
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	364
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	329
68.180.229.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	325
212.25.84.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	318
195.66.128.86	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	302
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	296
165.50.191.111		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	296
66.249.73.185	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	287
66.249.73.201	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	286
47.19.130.146	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	284
66.249.73.193	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	284
91.151.234.22	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	283
2.52.140.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	257
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	254
93.173.152.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	249
157.55.39.239	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	246
66.102.8.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	234
37.239.128.106	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	231

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	941
109.253.128.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	711
176.12.148.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	627
185.32.178.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	480
109.253.149.120	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.149.120	Block	338
46.19.85.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	324
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	308
176.12.138.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	295
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	285
176.12.142.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	273
46.19.85.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	272
82.80.42.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	251
109.253.142.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	249
46.121.130.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	248
77.127.84.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	247
37.26.147.148	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.148	Block	216
2.54.36.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	175
46.19.85.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	164
109.253.159.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	159
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	142
2.52.171.77	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.171.77	Block	138
84.108.38.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	132
46.19.86.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	106
2.52.11.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	91
109.253.140.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	84
109.253.157.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
37.26.147.187	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.187	Block	56
109.253.139.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	40
84.229.35.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
2.54.59.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	27
176.12.151.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
176.12.148.46	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.148.46	Block	23
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	19
5.9.45.155	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.9.45.155	Block	19
185.32.178.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	17
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	16
185.32.178.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	15
37.26.147.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
85.250.247.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	12
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	11
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
46.19.86.105	Israel	147.237.0.19	madim.atal.idf.i	Multiple Unauthorized URL Access from 46.19.86.105	Block	10
109.226.15.199	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	9
79.179.153.167	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	8
94.153.10.249	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15081-he/	Block	8
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.i	Multiple Unauthorized URL Access from 212.179.21.194	Block	8
147.235.236.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	8