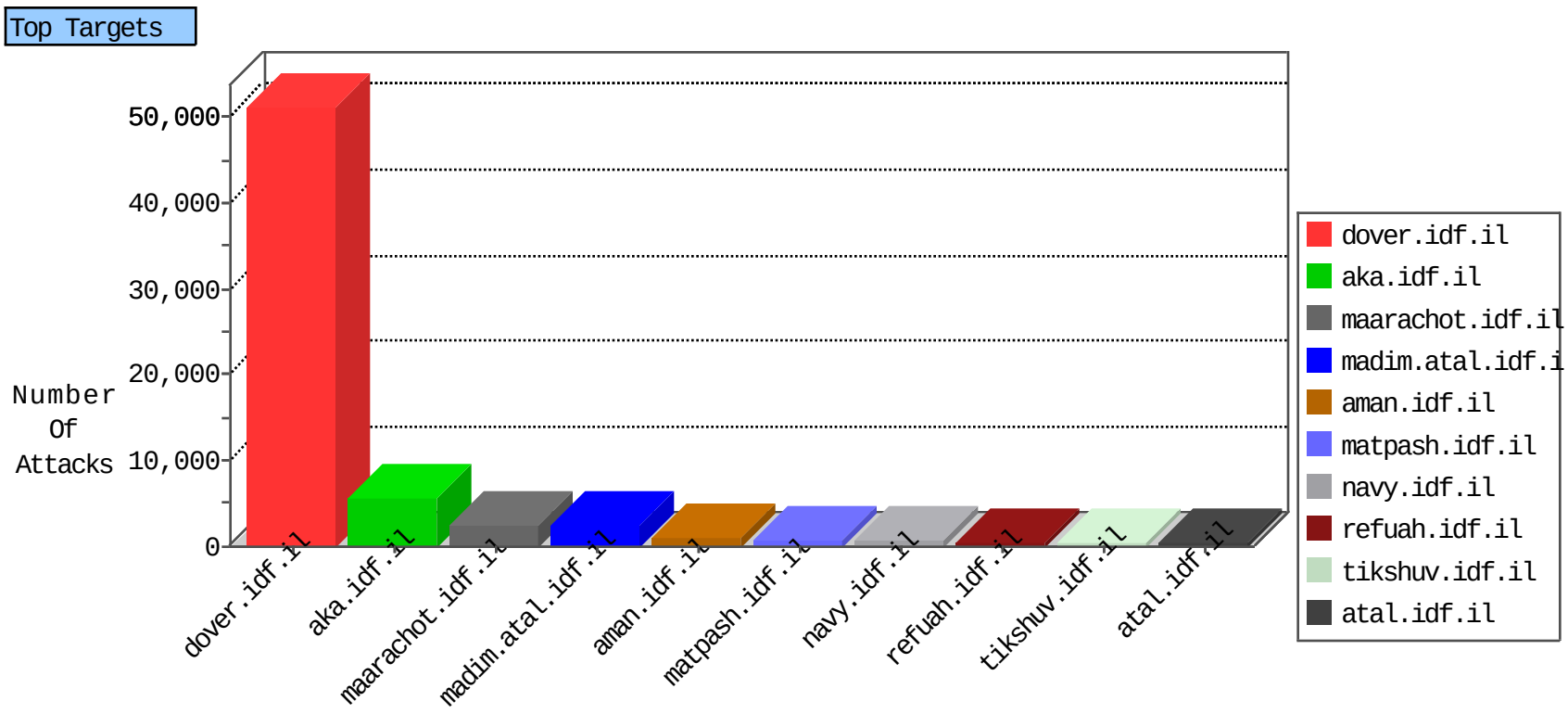
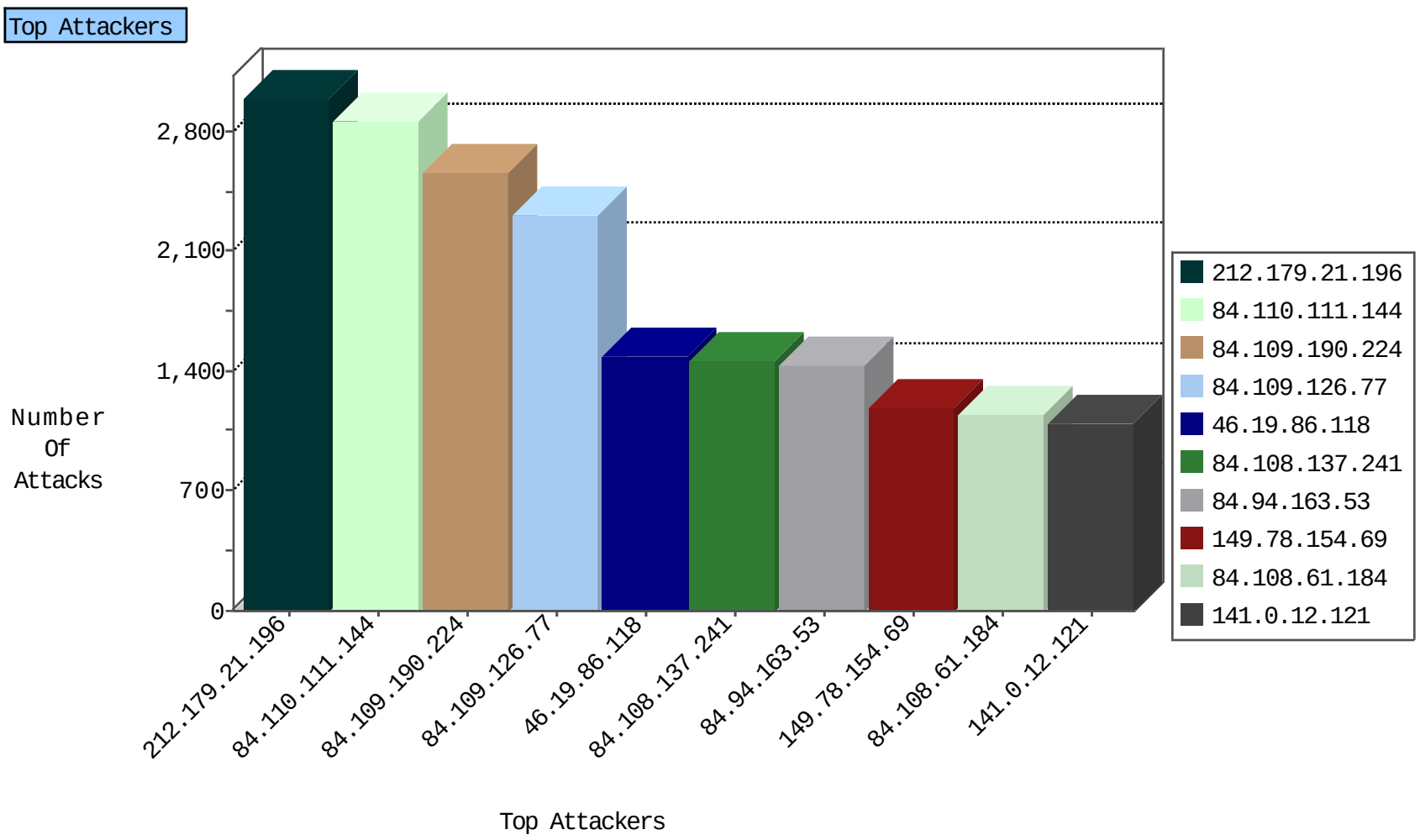
05-22-2015-00:00:05 to 05-23-2015-00:00:05

IDF Under Attack Daily Report





05-22-2015-00:00:05 to 05-23-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
220.181.108.161	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	81751
220.181.108.139	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	28107
220.181.108.85	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	19427
220.181.108.96	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	13413
78.108.161.226	Lebanon	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	6621
220.181.108.160	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	6486
220.181.108.166	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	5048
154.121.251.200		147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2266
82.166.20.8	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	485
46.117.20.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	459
5.22.129.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	410
77.125.220.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	339
79.179.108.175	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	336
87.68.209.127	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	325
220.181.108.102	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	284
220.181.108.149	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	273
185.3.146.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	250
220.181.108.118	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	228
79.181.190.17	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
87.68.218.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
84.228.222.58	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	150
37.142.4.90	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
208.54.80.212	United States	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	142
79.179.24.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	135
5.28.160.143	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	118
46.120.158.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
89.138.246.243	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	107
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	104
176.12.141.139	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
132.70.66.13	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
2.54.7.127	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	90
176.12.136.219	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
85.250.187.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	85
84.228.144.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
2.54.11.39	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
93.172.196.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
132.66.234.47	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
87.68.78.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
46.19.85.168	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
95.86.68.62	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	72
5.102.254.220	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
93.173.172.50	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
185.32.178.167	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	65
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	34
184.96.116.70	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	32
114.143.221.234	India	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	29
79.180.197.73	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
69.169.42.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15

05-22-2015-00:00:05 to 05-23-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.110.111.144	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2861
84.109.190.224	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2560
84.109.126.77	Israel	147.237.77.170	maarachot.idf.il	DVRep_P-N_40-59	Permit	2318
84.94.163.53	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1431
84.108.61.184	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1143
84.111.24.159	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	983
84.108.137.241	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	777
84.110.111.70	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	727
84.108.137.241	Israel	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	682
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	464
84.94.163.167	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	342
84.94.41.65	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	316
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	163
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	145
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	131
84.94.45.169	Israel	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	126
84.108.39.159	Israel	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	71
109.66.37.118	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	37
84.108.78.58	Israel	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	37
74.222.5.196	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	27
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
84.108.78.69	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	19
46.121.81.86	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	18
79.183.23.192	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	16
209.147.144.7	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
109.65.161.31	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
84.111.240.146	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
64.69.65.152	United States	147.237.77.170	maarachot.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	10
79.181.102.113	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
64.69.65.152	United States	147.237.77.170	maarachot.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	9
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	8
79.177.172.55	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
93.173.9.193	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
37.142.99.162	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
84.111.24.80	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	7
84.109.152.21	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
87.69.219.9	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.188	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	6
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
84.111.158.15	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	6
62.90.202.62	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5

05-22-2015-00:00:05 to 05-23-2015-00:00:05

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	153
108.174.151.109	United States	147.237.77.233	atal.idf.il	SERVER-WEBAPP Mambo upload.php access	109
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	12
5.108.32.118	Saudi Arabia	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	12
154.121.251.200		147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
66.249.64.168	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	6
66.249.75.68	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
176.12.140.18	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.48	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.51	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
43.255.188.134	Japan	147.237.8.46	e.chinuch.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
43.255.188.134	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.134	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	3
23.245.26.156	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
154.121.251.200		147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	3
43.255.188.132	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.73.217	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
61.240.144.65	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
183.136.216.3	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.233	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.245	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.245	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
183.136.216.3	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.245	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.131	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
176.12.137.138	Israel	147.237.72.166	aka.idf.il	GPL SCAN myscan	2
43.255.188.134	Japan	147.237.72.217	e.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
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.245	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
183.136.216.3	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.18	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
183.136.216.3	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2

05-22-2015-00:00:05 to 05-23-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3000
46.19.86.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1492
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1179
141.0.12.121	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1101
141.0.13.108	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	774
46.19.85.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	624
84.108.232.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	607
77.107.74.43	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	579
68.194.246.181	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	574
222.169.15.150	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	564
204.93.58.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	562
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	549
95.86.100.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	506
63.141.217.27	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	476
37.26.147.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	437
149.78.97.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	414
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	397
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	369
46.117.1.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	340
5.108.3.200	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	339
2.54.143.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	333
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	292
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	290
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	278
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	278
93.173.169.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
199.36.184.224	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	250
164.97.245.84	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	226
177.198.34.147	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	210
108.34.139.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	208
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	208
94.159.229.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	207
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	206
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	205
66.171.228.201	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	199
80.246.130.142	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	189
140.163.254.156	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	187
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	187
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	184
93.126.188.111	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	181
37.26.147.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	177
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	177
37.228.104.150	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	174
212.143.144.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	168
176.228.64.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	160
187.234.248.39	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	159
89.139.188.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156
188.165.15.105	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	144
78.108.161.226	Lebanon	147.237.0.34	tikshuv.idf.i	First packet isn't SYN	drop	drop	143
187.233.146.104	Mexico	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	140

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.16.196	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.16.196	Block	701
46.19.85.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	636
109.253.140.35	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.140.35	Block	438
37.142.222.48	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.142.222.48	Block	251
109.65.195.124	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.65.195.124	Block	154
46.19.86.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	126
108.174.151.109	United States	147.237.77.233	atal.idf.il	PHP Attempt	Block	109
79.179.108.175	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.179.108.175	Block	93
79.177.17.214	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.177.17.214	Block	58
46.19.85.231	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.231	Block	45
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	38
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	24
125.65.46.131	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.46.131	Block	21
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	19
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	17
108.174.151.109	United States	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 108.174.151.109	Block	17
95.86.66.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	16
67.84.218.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	15
109.253.159.166	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.159.166	Block	14
149.78.178.17	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	13
85.250.69.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
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	13
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	12
91.214.98.33	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	12
5.102.254.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	12
79.179.15.121	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	12
2.54.96.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
109.65.14.73	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 109.65.14.73	Block	10
109.65.14.73	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.65.14.73	Block	10
109.65.14.73	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 109.65.14.73	Block	10
188.120.150.42	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	8
93.173.28.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
178.137.166.68	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	8
94.159.169.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
37.26.148.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
109.65.14.73	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 109.65.14.73	Block	7
84.171.129.225	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
95.86.100.203	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
109.65.14.73	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.65.14.73	Block	7
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
109.67.251.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
66.249.73.217	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.73.217	Block	6
109.67.102.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
5.29.117.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
109.67.37.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
109.253.141.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
87.69.160.116	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	6
89.138.192.178	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 89.138.192.178	Block	5
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	5
207.46.13.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5