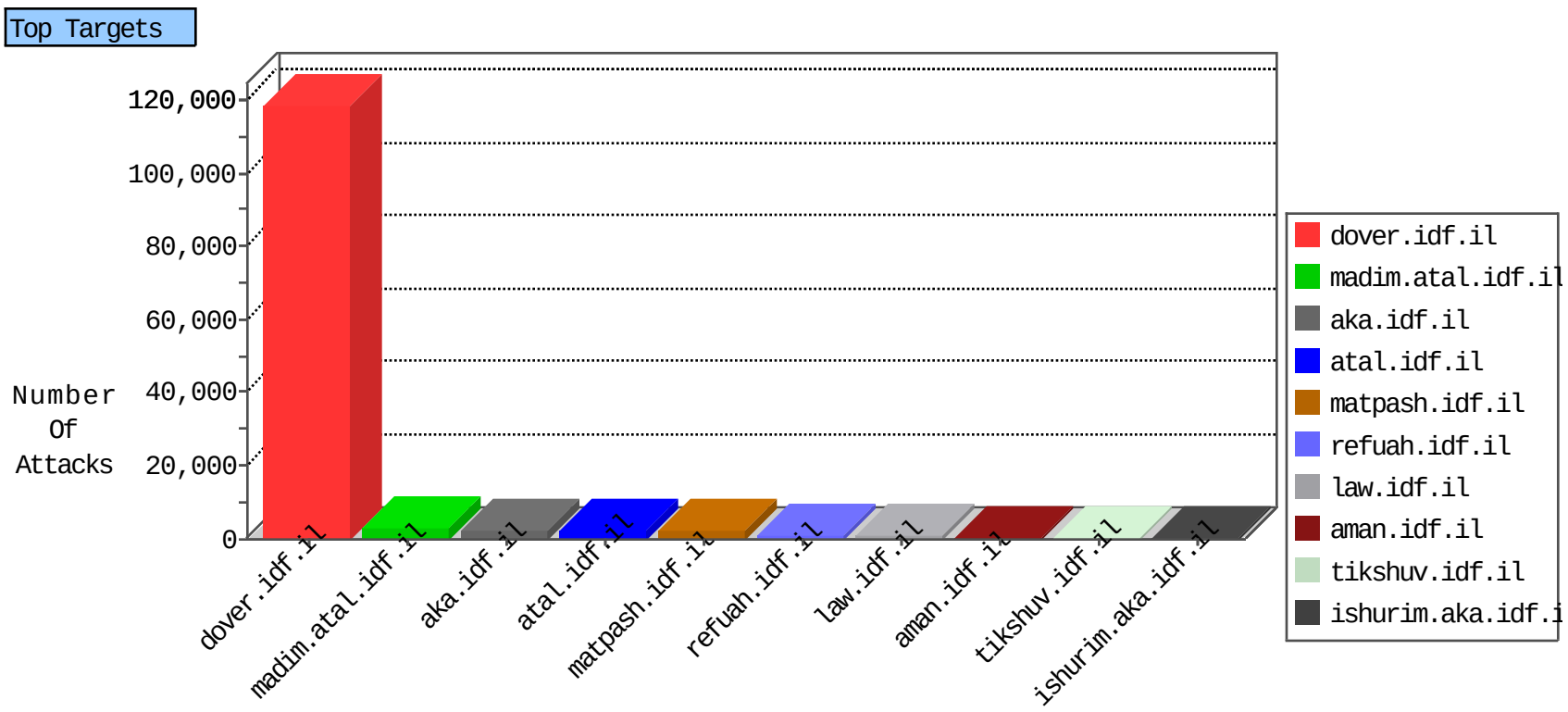
06-16-2015-00:00:03 to 06-17-2015-00:00:03

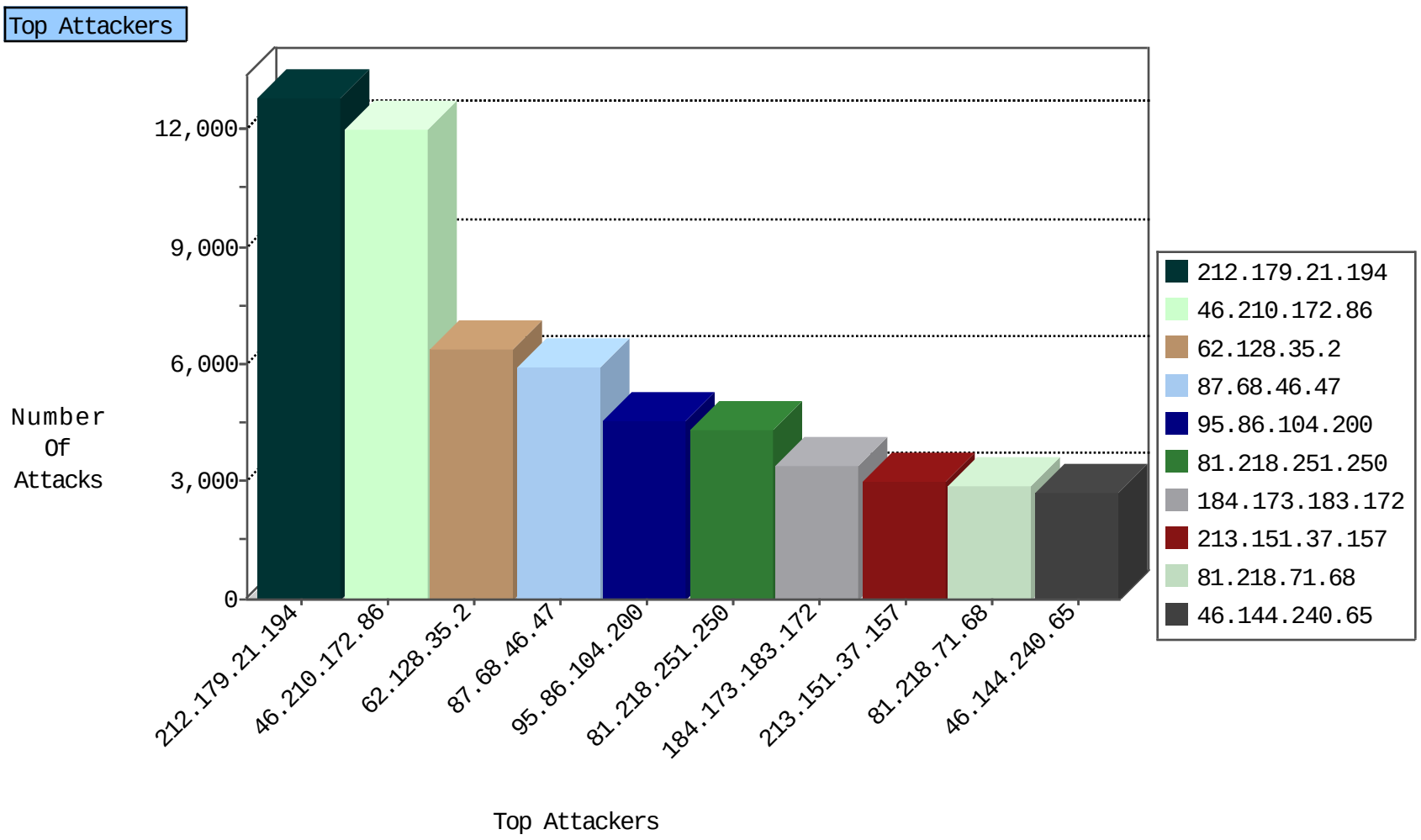
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

06-16-2015-00:00:03 to 06-17-2015-00:00:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
78.95.210.117	Romania	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	12760
176.67.59.140	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3301
85.250.140.105	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3111
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	629
220.181.108.143	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	578
46.121.248.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	493
84.108.166.88	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	397
78.95.210.117	Romania	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	396
62.128.35.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	374
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	350
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	320
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	307
79.177.229.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	285
78.95.210.117	Romania	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	268
176.12.151.244	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
46.120.231.171	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	228
220.181.108.76	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	218
2.52.22.7	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
213.151.57.77	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
77.127.220.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
84.108.132.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
79.176.174.160	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
80.246.136.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	145
199.190.46.37	Satellite Provider	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	141
185.32.178.193	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	119
46.117.137.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
185.32.178.124	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
46.120.31.40	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
2.52.53.56	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
84.228.255.41	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
213.151.35.218	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
37.26.147.200	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
185.32.178.193	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
84.94.47.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
46.116.224.31	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
46.121.102.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
77.125.75.71	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
84.94.32.197	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	89
84.228.170.195	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
2.54.46.154	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
37.187.157.108	France	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	82
185.32.178.213	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
46.19.86.98	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
109.253.143.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	79
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	75
46.19.86.207	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
149.78.102.127	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
46.19.85.52	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
46.117.45.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69

06-16-2015-00:00:03 to 06-17-2015-00:00:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	1694
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	625
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	430
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	252
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	194
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	193
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	113
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	20
79.182.129.44	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
81.218.251.250	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
176.56.61.11	United Kingdom	147.237.77.170	maarachot.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	12
81.218.251.252	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
31.13.163.43	Palestinian Territory, Occupied	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
192.116.177.202	Israel	147.237.77.243	mobile.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
87.68.56.144	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
192.116.197.84	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
93.173.168.155	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	6
79.181.222.137	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	5
85.250.140.105	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
213.139.52.106	Jordan	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5
198.240.130.75	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	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	5
192.114.7.2	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
87.68.214.35	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	4
114.24.54.86	Taiwan	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	4
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.234	halag.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	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4

06-16-2015-00:00:03 to 06-17-2015-00:00:03

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	89
37.26.147.182	Israel	147.237.77.176	matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	32
197.40.144.110	Egypt	147.237.77.216	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	29
85.250.140.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	11
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	10
197.40.144.110	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP awstats access	9
154.121.251.117		147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	4
109.65.173.39	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	4
154.121.251.117		147.237.77.216	dover.idf.il	GPL WEB_SERVER WEB-PHP phpinfo access	4
197.40.144.110	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP client negative Content-Length attempt	4
154.121.251.117		147.237.77.216	dover.idf.il	SERVER-WEBAPP WebDAV search access	4
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
120.40.157.95	China	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	3
197.40.144.110	Egypt	147.237.77.216	dover.idf.il	GPL WEB_SERVER webalizer access	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
43.255.188.130	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	3
197.40.144.110	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP webalizer access	3
61.148.116.114	China	147.237.77.74	law.idf.il	GPL SCAN nmap TCP	2
66.249.65.26	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.168	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.79.86	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
154.121.251.117		147.237.77.216	dover.idf.il	ET SCAN w3af Scan In Progress ARGENTINA Req Method	2
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
197.40.144.110	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP WEB-INF access	2
217.66.243.125	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
197.40.144.110	Egypt	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	2
197.40.144.110	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	2
154.121.251.117		147.237.77.216	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
2.54.145.98	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.198	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.77.227	e.hamaz.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
189.84.21.229	Brazil	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
43.255.188.130	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
125.19.7.107	India	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.79.73.216	Netherlands	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.205.34.201	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.183.165.86	Thailand	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.188.132	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
154.121.251.117		147.237.77.216	dover.idf.il	WEB-FRONTPAGE /_vti_bin/ access	1
31.168.229.154	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.109.61	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.73.185	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

06-16-2015-00:00:03 to 06-17-2015-00:00:03

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.i	First packet isn't SYN	drop	drop	12748
46.210.172.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11967
62.128.35.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6406
87.68.46.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5943
95.86.104.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4567
81.218.251.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4330
213.151.37.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3027
81.218.71.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2897
46.144.240.65	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2744
85.250.140.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2229
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1851
212.143.186.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1240
199.190.46.37	Satellite Provid	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	860
46.120.72.237	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	745
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	741
222.169.15.146	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	659
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	619
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	574
213.204.127.33	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	539
31.168.135.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	496
154.121.251.117		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	465
132.66.40.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	404
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	396
77.125.141.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	390
37.237.152.17	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	387
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	378
68.180.229.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	372
81.218.50.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	371
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	356
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	351
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	330
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	328
212.143.3.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	327
82.145.211.17	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	300
54.187.55.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	287
77.125.12.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	274
37.237.140.48	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	274
46.210.174.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	264
200.53.156.160	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	258
84.94.32.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	248
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	245
93.173.152.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	237
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	236
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	236
2.52.146.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	230
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	230
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	230
207.46.13.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	208
85.57.178.101	Spain	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	201
2.54.35.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	200

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
185.32.178.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	511
176.12.144.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	494
109.64.198.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	314
46.117.38.177	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.38.177	Block	271
2.52.20.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	256
176.12.145.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	154
185.32.178.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	152
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.165	Block	151
2.52.180.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	126
185.32.178.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	124
37.26.147.183	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.183	Block	101
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.21	Block	84
109.253.132.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
2.54.43.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
46.19.86.1	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.1	Block	58
46.121.78.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
46.19.85.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
2.54.15.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
109.253.138.75	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.138.75	Block	50
46.19.85.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
37.26.146.234	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.234	Block	42
79.180.38.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
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	35
109.226.15.199	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	20
132.65.125.80	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	15
176.12.140.170	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.140.170	Block	15
109.226.15.199	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	13
37.26.147.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
200.53.156.180	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
176.12.150.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
77.125.15.43	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	11
154.121.251.117		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 154.121.251.117	Block	11
109.66.101.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
31.168.69.70	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	10
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/size103x103/sip_storage	Block	10
109.64.39.54	Israel	147.237.77.170	maarachot.idf.il	Post Request - Missing Content Type from 109.64.39.54	Block	10
41.137.68.5	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.137.68.5	Block	10
93.173.245.90	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	10
200.53.156.160	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	9
93.173.245.90	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	9
79.183.51.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
149.88.94.95	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
213.151.37.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
2.54.18.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
85.64.23.57	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 85.64.23.57	None	7
176.12.144.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	6
109.186.191.0	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 109.186.191.0	Block	6

06-16-2015-00:00:03 to 06-17-2015-00:00:03