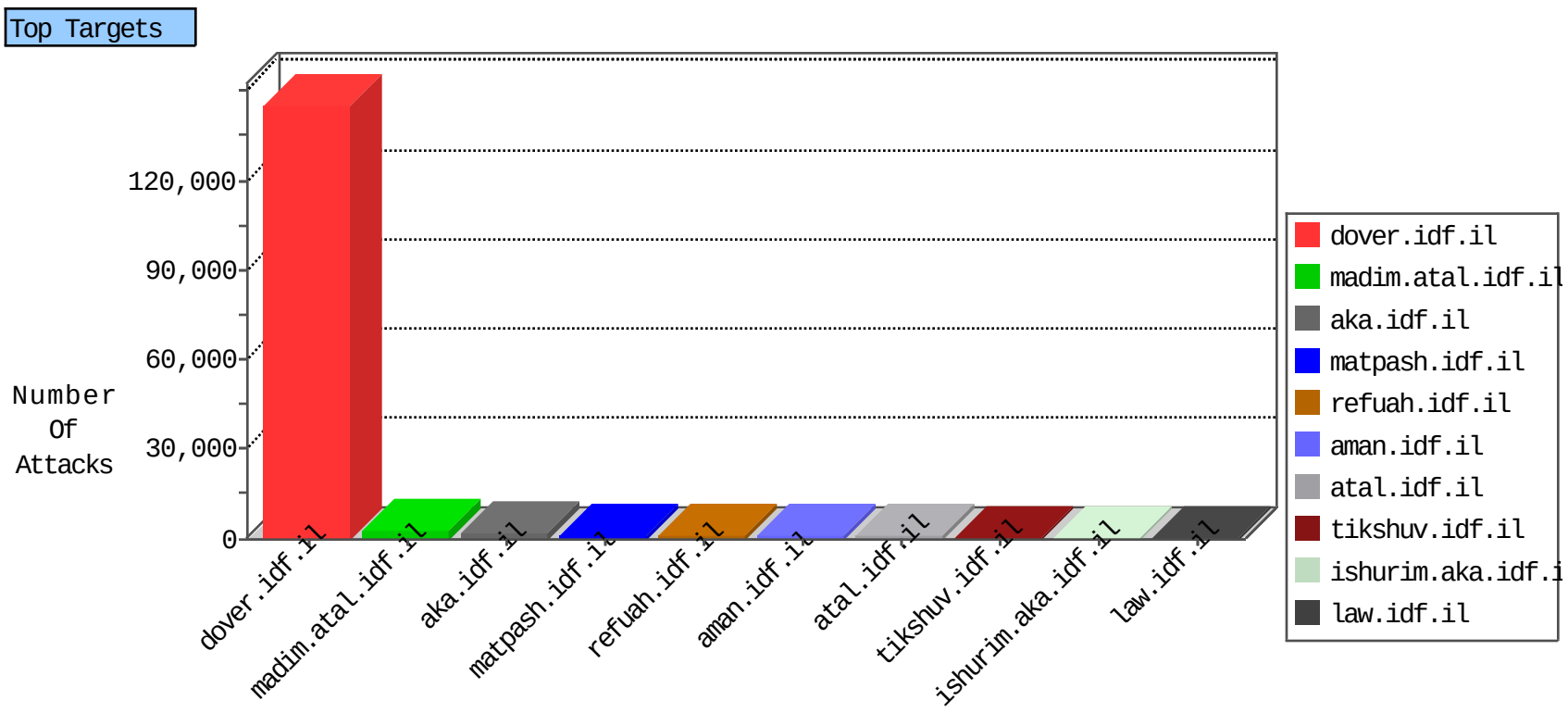
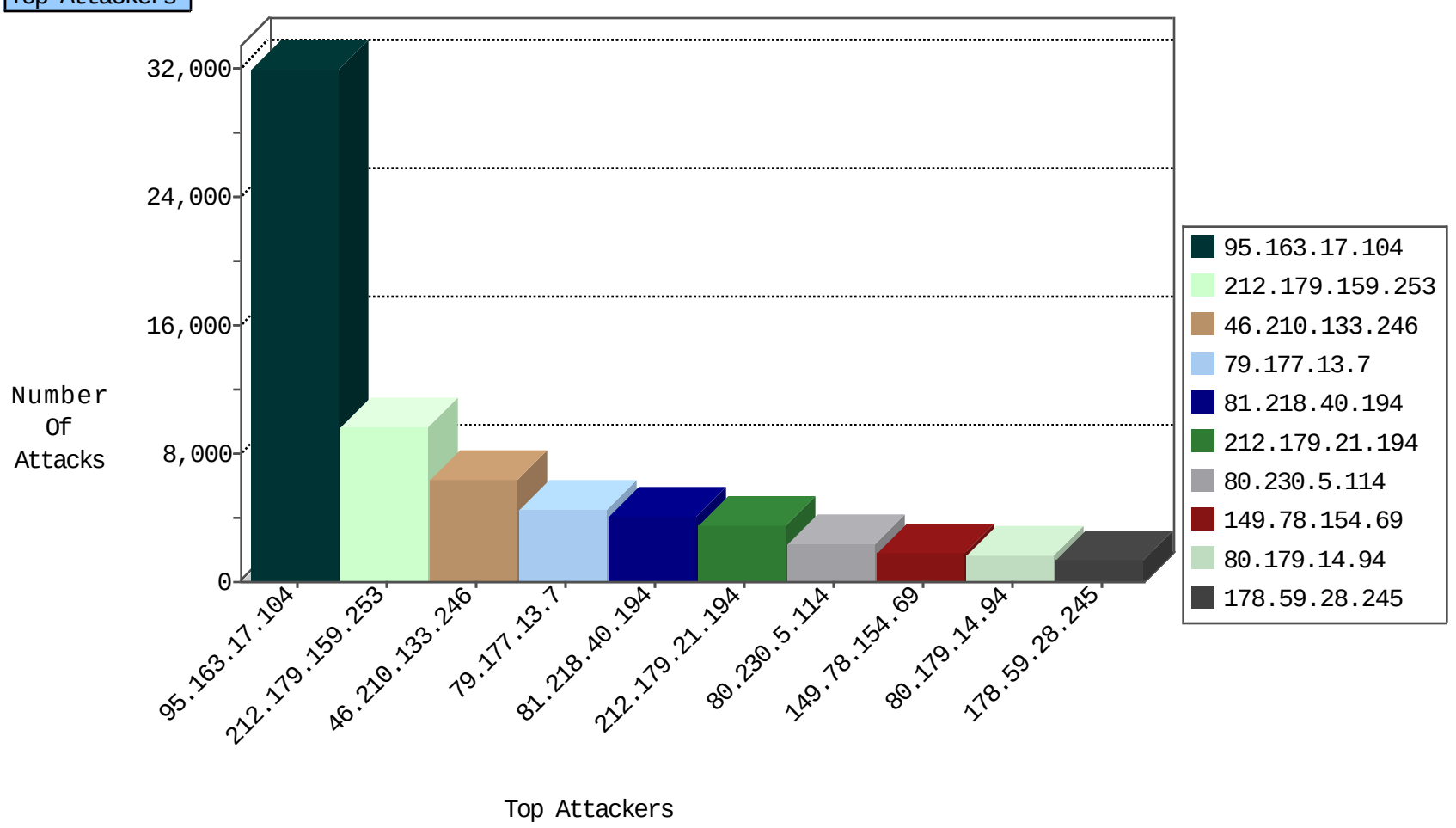
07-07-2015-00:00:03 to 07-08-2015-00:00:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



07-07-2015-00:00:03 to 07-08-2015-00:00:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5780
84.109.0.86	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3141
54.72.73.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2897
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2792
84.108.171.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2535
95.232.210.221	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2058
89.138.79.233	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1161
213.244.123.75	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	953
84.109.154.171	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	589
5.28.160.179	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	513
46.120.137.166	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	479
79.178.34.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	465
79.177.190.176	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	452
79.179.167.87	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	443
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	432
5.102.254.227	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	405
62.0.34.177	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	404
79.176.177.7	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	391
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	300
109.66.125.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	291
84.229.184.183	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	280
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
185.4.252.171	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	238
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	221
93.172.164.13	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	200
46.121.102.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
79.179.175.234	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	190
46.120.223.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
192.115.141.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
79.176.165.87	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
79.182.12.80	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
87.68.22.250	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
5.29.117.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
46.120.34.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
85.64.93.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
109.65.140.76	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	134
77.127.161.12	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
46.121.108.57	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125
37.142.4.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	123
46.120.173.145	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	122
109.67.206.237	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
109.67.18.238	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	106
85.65.217.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
5.28.147.212	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
5.102.254.227	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	96
85.64.50.78	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
87.69.139.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
79.178.102.225	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	87
79.178.13.99	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85

07-07-2015-00:00:03 to 07-08-2015-00:00:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.214.28.183	Germany	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	24
85.214.28.183	Germany	147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	24
192.115.130.253	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	15
95.163.17.104	Russian Federation	147.237.77.216	dover.idf.il	12371: TCP: Hulk DDoS Tool	Block	7
79.181.117.238	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
87.68.38.226	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.182.185.81	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
87.68.97.93	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
82.80.166.244	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
62.90.192.168	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
80.179.6.248	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
62.90.235.123	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
178.22.66.120	Switzerland	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
178.22.66.120	Switzerland	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.19.85.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
80.179.225.230	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
63.238.139.240	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
192.117.159.82	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
5.29.29.188	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.65.149.248	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
93.172.164.13	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
78.47.123.24	Germany	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	3
93.172.164.109	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.99	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.179.163.56	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.57.145.77	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.57.162.156	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.186.184.33	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.86.125	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.102.254.202	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.179.225.42	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.149	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
172.10.254.23	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.226.45.159	France	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.179.216.97	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.164	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.67.50.101	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.156	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.166.114.56	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.252.167.167	Turkey	147.237.77.74	law.idf.il	12373: HTTP: WordPress admin Login	Block	2
109.64.43.63	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
185.32.178.29	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.246.137.144	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.120.196.58	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.156	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.94.170.203	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.26.146.239	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.176.126.166	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.185	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

07-07-2015-00:00:03 to 07-08-2015-00:00:03

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	55
85.214.28.183	Germany	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	20
66.249.67.81	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	11
193.238.152.34	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	5
193.238.152.34	Ukraine	147.237.77.216	dover.idf.il	SERVER-WEBAPP /_admin access	4
82.166.22.63	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
61.183.128.6	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	3
61.183.128.6	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	3
221.203.3.117	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.161	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
109.253.157.90	Israel	147.237.72.156	aman.idf.il	INDICATOR-SCAN myscan	2
218.87.111.107	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
218.65.30.107	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.77.226	www.chamatz.aka.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
87.69.241.127	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.67.73	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
109.253.157.90	Israel	147.237.72.156	aman.idf.il	GPL SCAN myscan	2
66.249.78.172	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
193.5.216.100	Switzerland	147.237.77.176	matpash.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
113.240.250.156	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
91.121.242.210	France	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.67.59	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	1
210.61.150.154	Taiwan	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
177.132.44.150	Brazil	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
2.54.180.29	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
104.167.112.16		147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 2048	1
218.65.30.107	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
196.47.173.21	Cote D'Ivoire	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.188.135	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
121.14.5.125	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
46.19.86.165	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
147.236.30.190	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.54	Netherlands	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.178.60.25	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.212.161	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.128	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
192.114.170.10	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
24.132.212.111	Netherlands	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
111.202.143.149	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
87.68.30.95	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.111.107	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1

07-07-2015-00:00:03 to 07-08-2015-00:00:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.163.17.104	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32098
212.179.159.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9644
46.210.133.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6371
79.177.13.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4462
81.218.40.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4082
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3332
80.230.5.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2320
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1852
80.179.14.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1705
178.59.28.245	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1360
2.54.53.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1242
192.118.64.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1107
32.97.110.58	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	1052
82.145.209.171	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1038
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	976
200.82.57.235	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	946
62.0.34.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	927
141.0.12.190	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	826
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	808
84.94.32.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	796
46.43.100.94	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	677
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	617
77.125.145.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	611
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	594
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	590
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	581
46.19.86.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	560
212.179.71.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	553
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	532
37.142.14.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	526
46.19.85.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	519
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	514
109.186.0.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	493
84.108.39.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	489
37.141.192.148	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	449
82.166.22.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	433
168.168.1.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	423
213.151.35.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	411
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	404
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	394
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	384
95.86.92.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	372
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	366
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	364
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	332
192.116.134.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	307
77.125.11.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	306
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	300
212.179.221.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	296
82.145.217.252	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	294

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.13.17.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	905
176.13.11.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	515
176.12.137.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	391
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	218
46.19.86.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	212
37.26.146.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	162
46.19.86.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	132
2.54.24.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	115
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	96
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	96
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	82
46.19.86.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	74
46.19.85.221	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.221	Block	66
109.253.149.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
176.12.136.71	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.136.71	Block	55
77.125.214.135	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$txtTo in my-kosher-kravi.idf.il/modules/messages/form.aspx	Block	47
2.52.57.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	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	44
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	39
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.137	Block	38
109.160.188.141	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.160.188.141	Block	37
109.253.134.12	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.134.12	Block	35
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	35
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	33
38.111.147.88	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 38.111.147.88	Block	25
109.253.144.100	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.144.100	Block	24
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	23
80.246.136.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
85.214.28.183	Germany	147.237.72.166	aka.idf.il	PHP Attempt	Block	20
77.125.137.49	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 77.125.137.49	Block	18
81.17.16.247	Switzerland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	15
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
95.86.72.25	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	14
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//library/manage/resource/getfilecontent.hh.asp	Block	12
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	12
46.229.164.100	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.100	Block	11
157.55.39.32	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.32	Block	11
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
185.32.178.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
113.176.94.97	Vietnam	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	9
176.13.19.14	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	Block	9
84.111.36.38	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	9
176.13.19.14	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.19.14	None	8
79.182.99.139	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.182.99.139	Block	8
159.224.160.157	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 159.224.160.157	Block	7
46.229.164.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.102	Block	7
84.94.176.72	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
149.88.79.76	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6

07-07-2015-00:00:03 to 07-08-2015-00:00:03