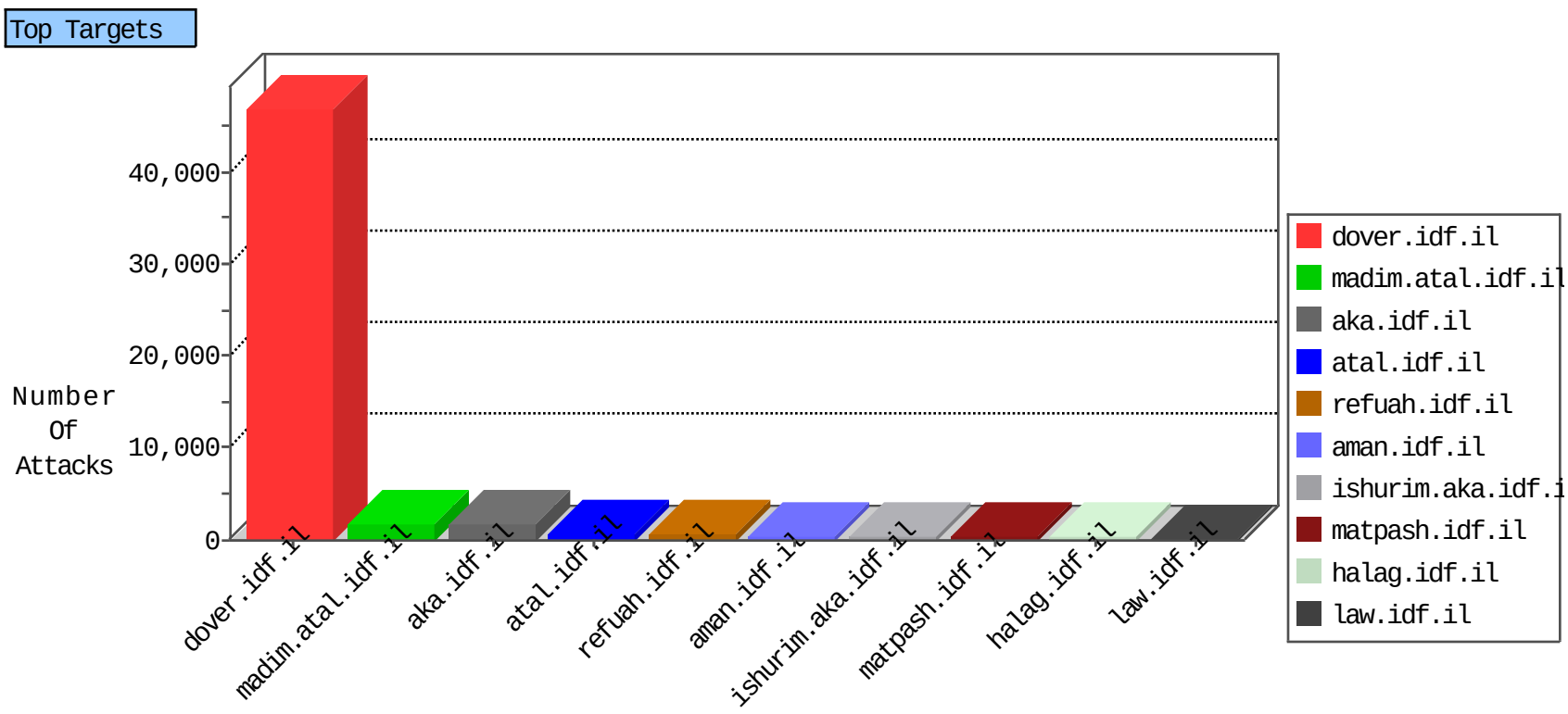
07-04-2015-00:00:08 to 07-05-2015-00:00:08

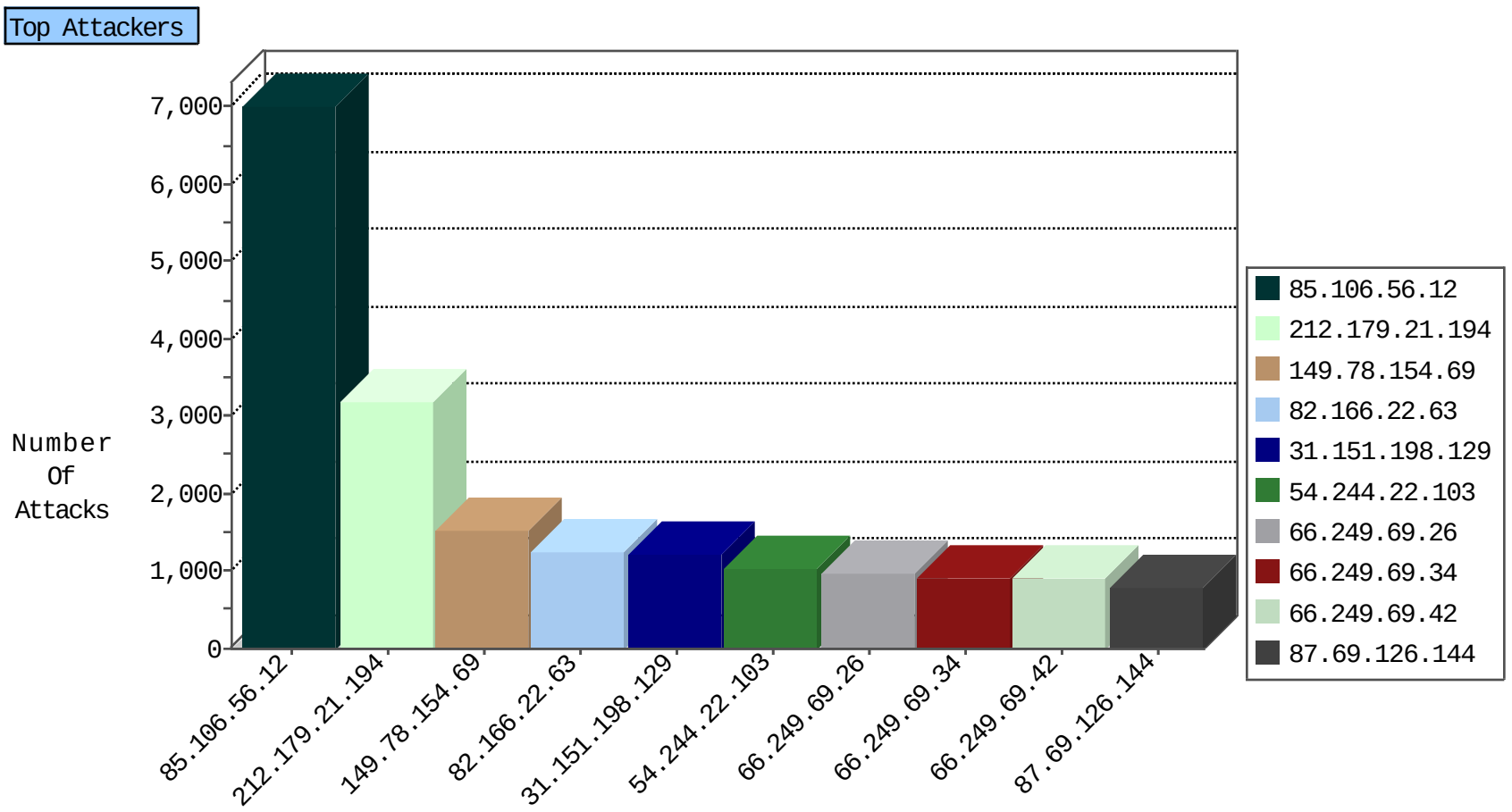
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

07-04-2015-00:00:08 to 07-05-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
89.138.255.165	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	2188
192.116.128.90	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1698
82.166.22.63	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	835
220.181.108.142	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	592
82.166.22.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	541
5.22.129.234	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	357
93.172.222.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	342
94.159.219.28	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	342
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	326
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	326
81.218.202.131	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	313
87.69.205.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	293
94.159.219.28	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	267
79.180.175.59	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	220
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
46.121.154.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
84.111.180.233	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	182
46.121.207.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
149.78.131.129	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
109.67.158.125	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
185.32.178.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	160
220.181.108.171	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	143
46.121.244.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
46.121.102.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
2.52.9.57	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	130
37.142.170.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
109.64.122.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
5.29.54.108	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	113
46.120.34.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
84.108.67.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
77.127.206.17	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
77.126.225.225	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
5.28.178.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	80
194.90.37.13	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	79
46.19.86.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
37.26.147.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	68
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
109.66.17.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	34
2.54.18.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	31
84.94.32.197	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	28
87.69.126.144	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	23
82.166.22.63	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
84.94.32.197	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
10.0.0.14		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
79.176.6.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
79.182.175.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
109.253.139.245	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
192.168.0.103		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
46.19.85.94	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12

07-04-2015-00:00:08 to 07-05-2015-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
103.228.1.242		147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	16
178.234.251.46	Russian Federation	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
82.166.22.63	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
46.19.85.135	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
79.181.60.69	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
149.88.26.232	United States	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
37.59.125.59	France	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	6
213.139.53.10	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
2.52.29.18	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.116.184.76	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
213.139.52.59	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.182.186.105	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.181.4.70	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.150	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.156	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.183.151.146	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
106.185.46.214	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.110.75.198	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.65.157.183	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
77.125.212.223	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
190.12.181.171	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.179.123.56	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.139.56.11	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.120.195.220	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.113	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.183.164.93	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.115	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.246	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.180.21.157	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.160.187.218	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.22.129.189	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
124.197.10.52	New Zealand	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
216.251.203.242	United States	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.95.83.134	Israel	147.237.0.15	kosher-kravi.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
162.210.196.130	United States	147.237.76.42	refuah.idf.il	C1000106: HTTP: majestic bot	Block	1
74.206.240.244	United States	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
85.250.236.107	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
213.57.111.2	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.142.166.15	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
5.28.160.179	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.179.199.94	Israel	147.237.76.200	eitan.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.120.202.26	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
91.121.169.194	France	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
79.182.185.220	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.26.148.205	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
172.82.176.68		147.237.77.74	law.idf.il	0854: HTTP: upload* Access	Permit	1
76.220.40.252	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
86.139.30.69	United Kingdom	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

07-04-2015-00:00:08 to 07-05-2015-00:00:08

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	47
85.99.44.212	Turkey	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	12
37.59.125.59	France	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	12
185.24.124.3	Lebanon	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.75.236	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
66.249.69.26	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
43.255.188.131	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.135	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	3
89.138.255.165	Israel	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	3
95.110.228.68	Italy	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
43.255.188.135	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.130	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
89.138.255.165	Israel	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.165	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	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	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
43.255.188.133	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.75.228	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
199.203.59.121	Israel	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.16	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.133	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.0.34	tikshuv.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
43.255.188.135	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.162	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.183	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
209.66.70.253	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
43.255.188.135	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2

07-04-2015-00:00:08 to 07-05-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
85.106.56.12	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6911
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3189
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1536
31.151.198.129	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1227
82.166.22.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1192
87.69.126.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	750
66.249.69.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	713
66.249.69.26	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	708
66.249.69.34	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	680
188.247.72.218	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	656
5.35.122.149	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	538
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	533
109.67.48.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	431
78.165.255.164	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	393
54.244.22.103	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	388
66.249.83.155	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	304
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	303
66.249.83.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	302
73.194.47.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	295
79.182.134.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	287
79.183.129.212	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	286
66.249.83.158	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	276
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	271
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	269
84.94.26.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	266
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	264
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	262
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	246
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	230
79.179.188.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	223
66.102.6.163	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	215
31.109.92.1	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	213
109.186.0.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	208
66.102.6.171	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	198
66.102.6.167	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	196
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	190
84.228.58.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	184
80.230.92.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	180
76.233.242.180	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	180
109.67.48.137	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	169
188.165.15.233	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	165
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	164
82.80.25.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	161
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	159
150.135.114.209	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	157
38.99.190.240	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	155
66.249.80.67	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	154
66.249.80.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	154
66.249.80.83	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	153
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	145

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.172.138.232	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 93.172.138.232	Block	727
2.54.170.52	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.170.52	Block	714
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	397
79.179.144.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	256
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	108
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	95
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	84
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	32
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	22
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	20
46.4.132.226	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.4.132.226	Block	15
79.176.31.132	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	14
104.243.32.242		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 104.243.32.242	Block	13
46.19.86.125	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	12
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	12
213.57.37.30	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	11
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	10
84.95.228.187	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
212.126.121.70	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	9
176.12.143.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
79.179.199.94	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	9
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	8
176.12.147.210	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
109.253.143.205	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	7
94.159.142.207	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 94.159.142.207	None	7
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.33	Block	7
77.125.160.185	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	7
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	6
178.137.162.15	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17155-en/	Block	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	6
46.229.164.98	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.98	Block	6
84.228.229.209	Bulgaria	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
85.250.112.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
164.138.112.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	5
27.126.184.125	Hong Kong	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
118.99.29.242	Hong Kong	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	5
27.126.188.85	Hong Kong	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
109.64.55.76	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
151.236.51.114	United Kingdom	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 151.236.51.114	Block	5
188.143.234.155	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/sendtofriend	Block	5
188.165.15.233	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.233	Block	4
84.108.208.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
46.120.45.239	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
103.237.74.250		147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	4
184.153.210.0	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.229.164.100	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.100	Block	4
157.55.39.17	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.17	Block	4
46.120.151.151	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
213.57.37.30	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	4
109.65.9.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4

07-04-2015-00:00:08 to 07-05-2015-00:00:08