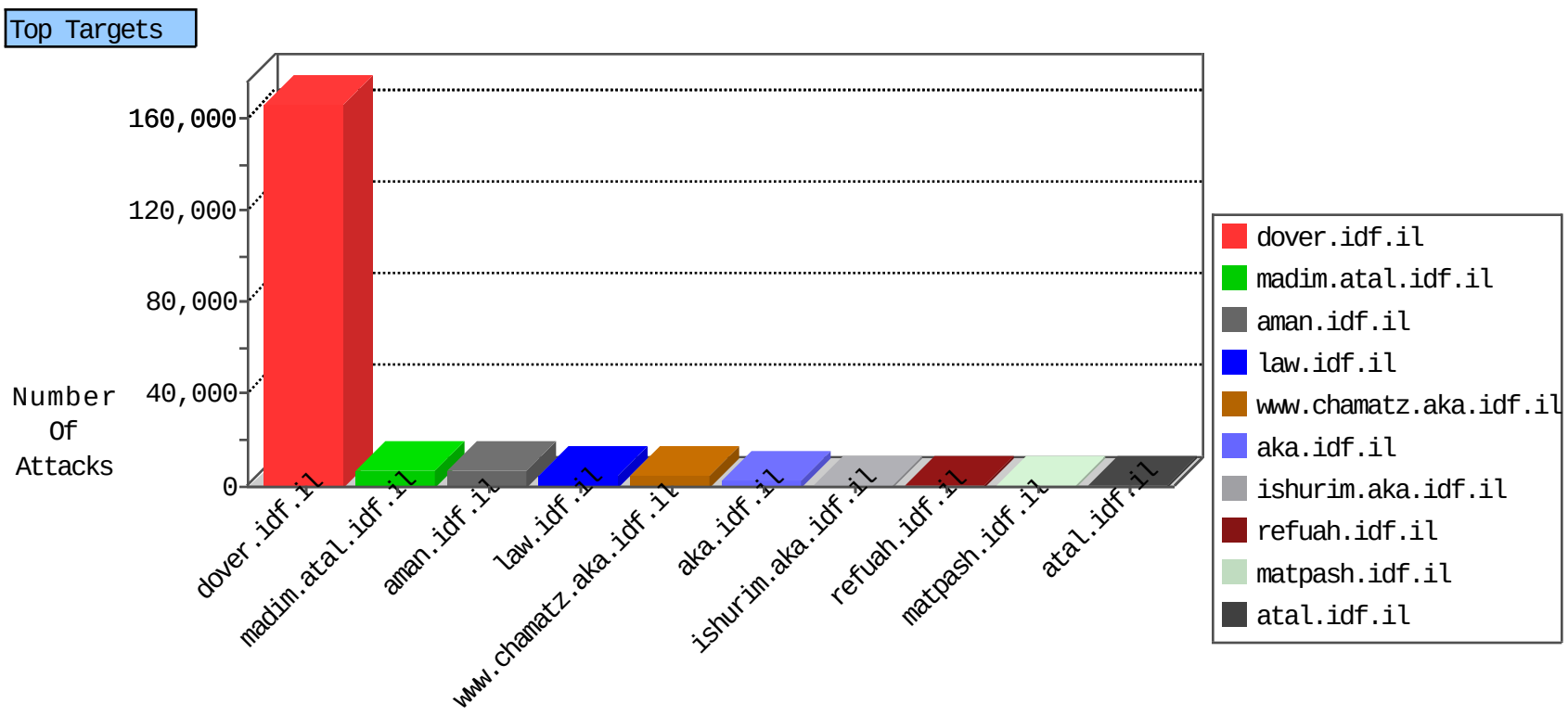
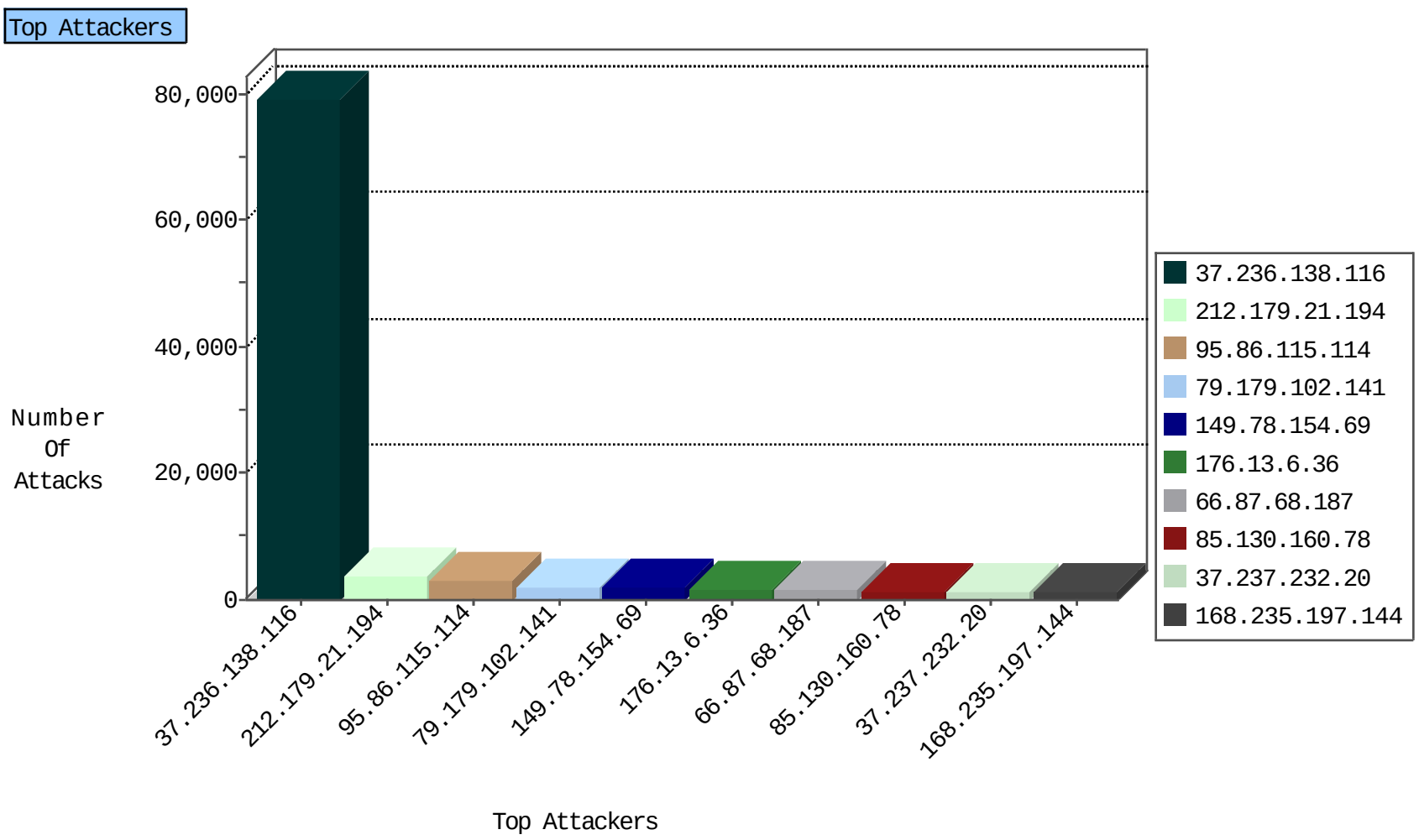
08-04-2015-00:00:09 to 08-05-2015-00:00:09

IDF Under Attack Daily Report





08-04-2015-00:00:09 to 08-05-2015-00:00:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
188.165.248.54	France	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	25486
66.249.67.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	24405
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22584
37.236.138.116	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	13318
66.249.65.199	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	10136
84.48.98.224	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6209
5.175.200.195	Germany	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	6161
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4923
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4751
5.175.200.177	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2586
109.67.206.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	2250
94.206.11.242	United Arab Emirates	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1961
80.246.136.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1925
149.78.80.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1520
212.117.154.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1388
176.223.84.223	Germany	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1361
37.236.138.116	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	995
176.13.21.215	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	852
176.223.81.49	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	675
212.25.84.200	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	586
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	463
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	459
94.249.246.175	Germany	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	454
149.88.108.216	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	412
85.250.183.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	377
176.223.84.116	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	343
109.64.27.201	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	334
77.125.5.12	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	319
82.211.18.69	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	314
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	312
77.125.115.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
37.142.64.105	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	308
85.64.124.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	299
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	295
77.125.78.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	293
46.120.53.199	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	291
37.142.64.135	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	285
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	283
85.64.62.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	265
79.181.120.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	248
84.108.118.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	248
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	240
85.64.2.106	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	239
93.173.26.20	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	230
82.81.160.227	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	225
31.168.230.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	207
46.117.161.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
95.86.125.155	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
37.142.64.79	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
109.65.175.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183

08-04-2015-00:00:09 to 08-05-2015-00:00:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.67.206.227	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	171
212.117.154.242	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	114
110.83.192.167	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	23
149.88.108.216	United States	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	21
82.205.101.145	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	20
110.83.192.167	China	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
85.250.124.48	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
89.138.249.244	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
192.116.177.194	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.179.121.186	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.116.128.247	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.40	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
93.173.37.56	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.108	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
80.179.37.248	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
181.55.174.204	Colombia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
197.40.152.198	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
211.59.8.170	Korea, Republic of	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
212.235.98.139	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.64.247.164	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
41.42.213.151	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
211.59.8.170	Korea, Republic of	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
184.57.129.196	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.126.6.27	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
95.86.117.20	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.185.146.161	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
5.102.254.213	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.211	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.42	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.32	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
5.29.108.158	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
76.79.128.66	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
217.55.146.162	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
31.154.178.141	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
192.117.13.162	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.178.106	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.57	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.57.194.71	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.198	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.162	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
83.130.107.129	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.160.169.104	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.250.10.136	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
202.67.43.41	Indonesia	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.88	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.65.81.13	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.183.198.189	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.64.178.9	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
194.176.105.165	United Kingdom	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

08-04-2015-00:00:09 to 08-05-2015-00:00:09

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	108
176.12.142.137	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
37.26.148.218	Israel	147.237.72.156	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
66.249.67.65	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	6
41.140.78.10	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP WEB-INF access	6
41.140.78.10	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	5
218.65.30.107	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	3
62.0.41.2	Israel	147.237.77.74	law.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
176.13.17.178	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
45.114.11.47		147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	3
218.65.30.107	China	147.237.77.74	law.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
45.114.11.46		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
79.176.115.168	Israel	147.237.72.156	aman.idf.il	portscan: TCP Distributed Portscan	2
218.65.30.107	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
41.140.78.10	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP PHP-CGI remote file include attempt	2
66.249.93.160	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.47		147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
191.97.37.15	Argentina	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
41.140.78.10	Morocco	147.237.77.216	dover.idf.il	ET WEB_SERVER auto_prepend_file PHP config option in uri	2
45.114.11.47		147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
201.76.122.4	Brazil	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
82.205.71.231	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
218.65.30.107	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
89.248.174.100	Netherlands	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
41.222.206.163	Seychelles	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
213.204.103.36	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.47		147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
121.34.176.28	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
201.76.122.4	Brazil	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
45.114.11.46		147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
45.114.11.47		147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
41.140.78.10	Morocco	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	2
194.63.142.85	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.218	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2

08-04-2015-00:00:09 to 08-05-2015-00:00:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.236.138.116	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	79000
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3518
95.86.115.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3053
79.179.102.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1991
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1774
66.87.68.187	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1459
85.130.160.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1283
37.237.232.20	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1271
168.235.197.144		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1228
46.210.130.51	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1085
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	903
95.86.119.169	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	858
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	857
46.19.86.216	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	827
82.145.216.97	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	793
66.87.68.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	725
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	665
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	622
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	617
66.249.67.53	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	616
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	607
95.86.120.53	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	594
66.249.67.59	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	578
66.249.67.65	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	572
188.165.15.152	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	538
31.44.141.117	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	532
66.249.84.182	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	521
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	518
71.201.156.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	510
66.249.84.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	508
84.94.199.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	505
66.249.84.188	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	490
2.54.39.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	476
79.179.148.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	437
46.5.86.167	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	417
85.250.92.188	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	413
2.54.49.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	412
37.237.205.60	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	410
95.86.65.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	400
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	383
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	375
105.188.93.127		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	354
31.154.178.141	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	347
37.239.128.18	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	329
68.180.228.112	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	326
212.179.57.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	323
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	304
83.130.107.129	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	303
5.102.254.213	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	299
5.102.254.213	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	293

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.13.6.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1712
176.13.17.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	793
185.32.179.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	758
2.52.2.160	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.2.160	Block	666
176.13.20.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	582
80.246.136.100	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 80.246.136.100	Block	546
5.102.254.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	324
46.19.86.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	278
176.13.21.239	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.21.239	Block	276
37.26.149.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	266
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	236
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	220
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	216
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	196
176.13.5.19	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.5.19	Block	186
176.12.139.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	136
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	70
37.26.147.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
87.69.126.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
188.165.15.152	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.152	Block	46
37.26.148.176	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	42
176.13.4.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	42
2.54.148.196	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	40
37.236.138.116	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.236.138.116	Block	38
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	38
185.32.179.165	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	30
2.54.172.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
109.65.33.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	20
5.29.151.24	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.29.151.24	Block	20
81.162.235.99	Ukraine	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.162.235.99	Block	18
81.162.235.99	Ukraine	147.237.76.86	navy.idf.il	PHP Attempt	Block	18
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	18
37.26.148.176	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	16
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	16
151.80.31.137	Italy	147.237.76.30	himush.idf.il	Unknown Parameter l in www.chimush.atal.idf.il/templates/sendtofriend/sendtofriend.aspx	None	14
94.159.196.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
176.12.144.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	14
176.13.13.91	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	14
80.246.139.95	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	12
213.151.61.104	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 213.151.61.104	Block	12
109.237.211.114	Netherlands	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	12
46.19.86.171	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.171	Block	12
109.65.191.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
62.0.34.177	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 62.0.34.177	Block	12
109.65.33.94	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	12
176.13.18.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
188.143.232.70	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.70	Block	10
146.185.31.218	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	10
79.178.199.35	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.178.199.35	Block	10