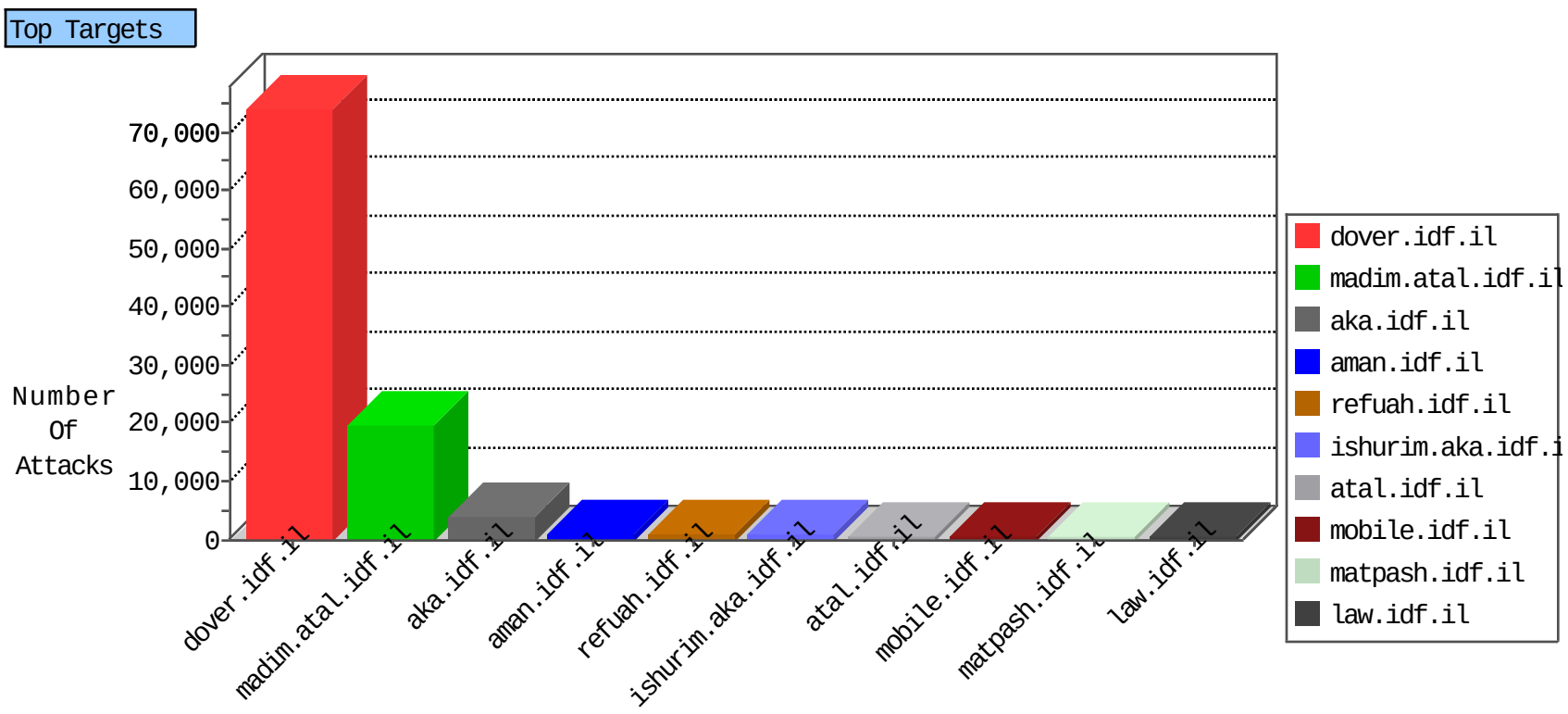
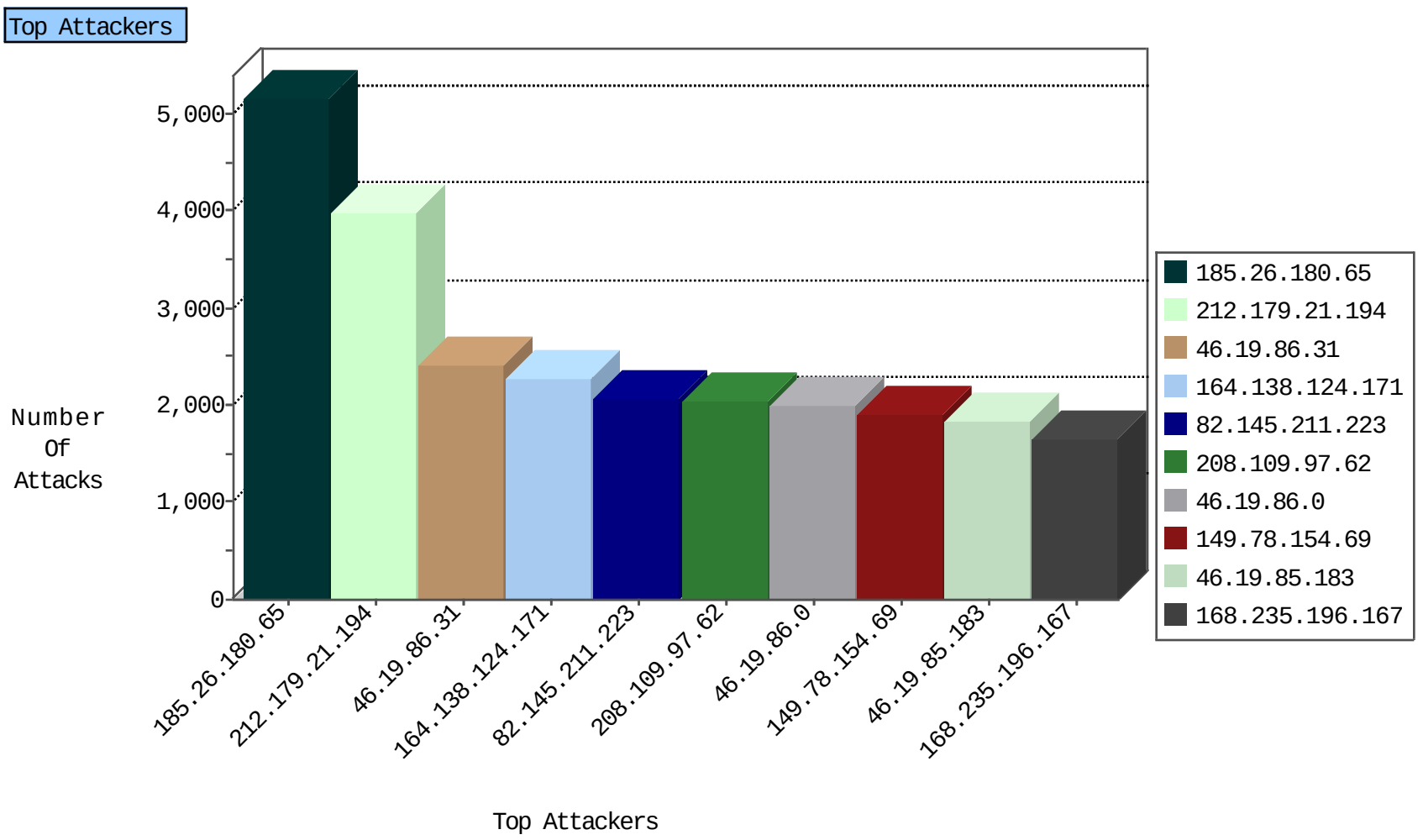
08-16-2015-00:00:06 to 08-17-2015-00:00:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-16-2015-00:00:06 to 08-17-2015-00:00:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
82.145.211.223	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	28754
108.91.116.139	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11472
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8275
79.178.179.109	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	5992
66.249.67.13	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3649
66.249.67.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3187
188.165.15.19	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2891
188.57.26.217	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2498
151.229.136.54	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1833
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1626
109.160.170.13	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1529
66.249.78.79	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	831
212.25.84.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	699
85.250.220.220	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	587
79.180.97.48	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	575
85.250.200.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	571
37.142.234.161	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	469
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	459
149.88.72.19	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	451
79.183.151.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	426
5.28.130.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	403
79.176.105.62	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	371
109.65.146.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	369
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	365
109.64.0.190	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	265
79.176.102.124	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	234
176.228.16.128	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	225
109.186.183.142	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	217
46.120.124.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	191
79.182.66.71	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	183
220.181.108.92	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	179
31.154.158.193	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	179
79.183.202.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	176
79.181.209.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
84.228.176.85	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
79.180.212.7	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	165
149.78.232.82	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
109.66.49.64	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	159
148.251.231.197	Germany	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	159
79.177.210.7	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
46.120.230.233	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
109.64.169.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	146
213.57.207.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	143
109.67.43.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
93.173.189.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	139
176.12.143.107	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	135
85.250.4.245	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	131
79.181.27.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
77.125.140.94	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	114

08-16-2015-00:00:06 to 08-17-2015-00:00:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
82.166.23.12	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	99
81.218.251.252	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	48
46.121.97.32	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	22
109.65.158.37	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	13
199.182.234.196	United States	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
199.182.234.196	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
46.19.85.236	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	11
77.125.74.229	Israel	147.237.0.15	kosher-kravi.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	10
84.108.44.205	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
46.120.17.179	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
188.97.2.205	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
176.13.15.177	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
37.75.215.31	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
82.166.25.122	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
69.91.112.52	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
31.168.92.115	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
111.107.162.240	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
82.166.23.74	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
194.177.198.27	Greece	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
188.161.16.202	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
31.154.5.110	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
46.19.85.242	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
193.106.206.10	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
109.64.171.156	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
107.14.56.128	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
180.191.111.30	Philippines	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
185.27.105.132	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
85.65.50.246	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.121.26.61	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.66.70.106	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
99.247.0.3	Canada	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
109.64.60.69	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
79.182.8.180	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
77.125.141.83	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
37.26.147.196	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
67.247.56.99	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
167.114.166.245	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
85.250.36.197	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
37.46.39.208	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
84.94.76.76	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.210.89.33	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
79.178.54.38	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.116.101.173	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.118	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
87.68.33.95	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
79.176.99.102	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
2.54.138.72	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
142.255.21.34	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
108.35.91.188	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1

08-16-2015-00:00:06 to 08-17-2015-00:00:06

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
148.251.231.197	Germany	147.237.77.216	dover.idf.il	SQL Injection - Select From	14
176.126.252.12	Romania	147.237.77.216	dover.idf.il	SQL Injection - Select From	14
2.52.47.204	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	9
148.251.231.197	Germany	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	8
194.177.198.27	Greece	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	7
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
89.138.222.236	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
148.251.231.197	Germany	147.237.77.216	dover.idf.il	ET SCAN Sqlmap SQL Injection Scan	4
91.219.236.218	Hungary	147.237.77.216	dover.idf.il	SQL Injection - Select From	3
209.222.8.196	United States	147.237.77.216	dover.idf.il	SQL Injection - Select From	3
213.151.53.29	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	3
185.22.183.202	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	3
186.219.208.174	Brazil	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
83.149.126.29	Netherlands	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	2
45.114.11.46		147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
116.24.169.42	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
109.67.164.253	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
148.251.231.197	Germany	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	2
45.114.11.46		147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
116.24.169.42	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
176.126.252.12	Romania	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	2
216.158.254.21	United States	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
176.126.252.12	Romania	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	2
108.61.99.31	United States	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	2
218.65.30.107	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
186.219.208.174	Brazil	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
213.57.211.35	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
94.23.30.53	France	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	2
199.203.59.121	Israel	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
103.3.236.13	Australia	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
209.222.8.196	United States	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
77.109.141.138	Switzerland	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	2
95.142.161.63	France	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	2
216.158.254.21	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
148.251.231.197	Germany	147.237.77.216	dover.idf.il	SQL waitfor delay function - possible SQL injection attempt	1
5.29.202.22	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.52.174	Netherlands	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
79.180.16.253	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.52.195	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.227.185	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
178.254.38.55	Germany	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
45.114.11.46		147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
111.26.188.229	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
84.108.24.168	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
74.82.194.10	Canada	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
189.202.241.84	Mexico	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
79.60.210.30	Italy	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1

08-16-2015-00:00:06 to 08-17-2015-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.26.180.65	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5157
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3720
164.138.124.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2277
82.145.211.223	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2040
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1894
168.235.196.167		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1652
208.109.97.62	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	1259
31.44.142.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1142
79.183.120.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1104
91.227.71.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	726
208.109.97.62	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	690
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	571
66.249.67.65	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	552
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	511
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	497
66.249.67.53	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	496
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	494
66.249.67.59	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	458
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	423
31.31.228.58	Czech Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	422
188.165.15.19	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	391
164.138.118.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	347
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	337
85.115.52.201	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	321
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	317
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	301
91.230.121.133	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	300
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	293
149.78.236.68	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	291
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
80.246.133.182	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	276
213.149.188.113	Cyprus	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	266
66.87.74.4	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	266
207.46.13.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	246
37.216.133.203	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	243
46.19.86.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	236
190.52.152.220	Paraguay	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	218
207.46.13.67	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	207
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	205
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	200
85.250.220.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	199
207.46.13.36	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	195
82.80.198.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	195
89.138.231.197	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	187
79.183.117.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	182
79.180.196.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	181
89.68.223.26	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	180
31.44.137.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	177
95.86.104.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	177
70.199.67.110	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	170

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.31	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.31	Block	2295
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1828
80.246.136.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1652
46.19.86.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1614
176.13.17.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1592
79.176.2.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1529
87.69.20.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1502
176.13.13.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	950
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	852
46.19.86.38	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.38	Block	834
46.19.86.102	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.102	Block	650
46.210.206.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	625
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	580
80.246.136.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	577
176.12.136.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	400
2.54.24.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	396
46.19.86.0	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.0	Block	374
95.211.226.36	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	320
176.12.148.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	292
176.12.143.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	212
176.12.142.177	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.142.177	Block	196
176.13.2.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	162
176.12.146.55	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.146.55	Block	136
176.228.86.60	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	100
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	96
2.52.133.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	84
2.54.39.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	76
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.201.224.176	Block	76
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	68
46.121.246.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.246.225	Block	68
149.78.40.163	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 149.78.40.163	Block	68
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	64
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	56
149.88.77.182	United States	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	56
192.114.23.18	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 192.114.23.18	Block	52
46.19.86.100	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	52
52.27.237.147	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	44
2.54.182.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	44
213.151.49.244	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	36
79.181.133.244	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	36
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	36
62.90.5.212	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	36
46.19.86.127	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	32
84.109.241.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	32
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	32
79.182.205.58	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.182.205.58	Block	28
188.165.15.19	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.19	Block	28
84.94.184.149	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
5.102.254.6	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.102.254.6	Block	28
77.127.195.18	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 77.127.195.18	Block	28