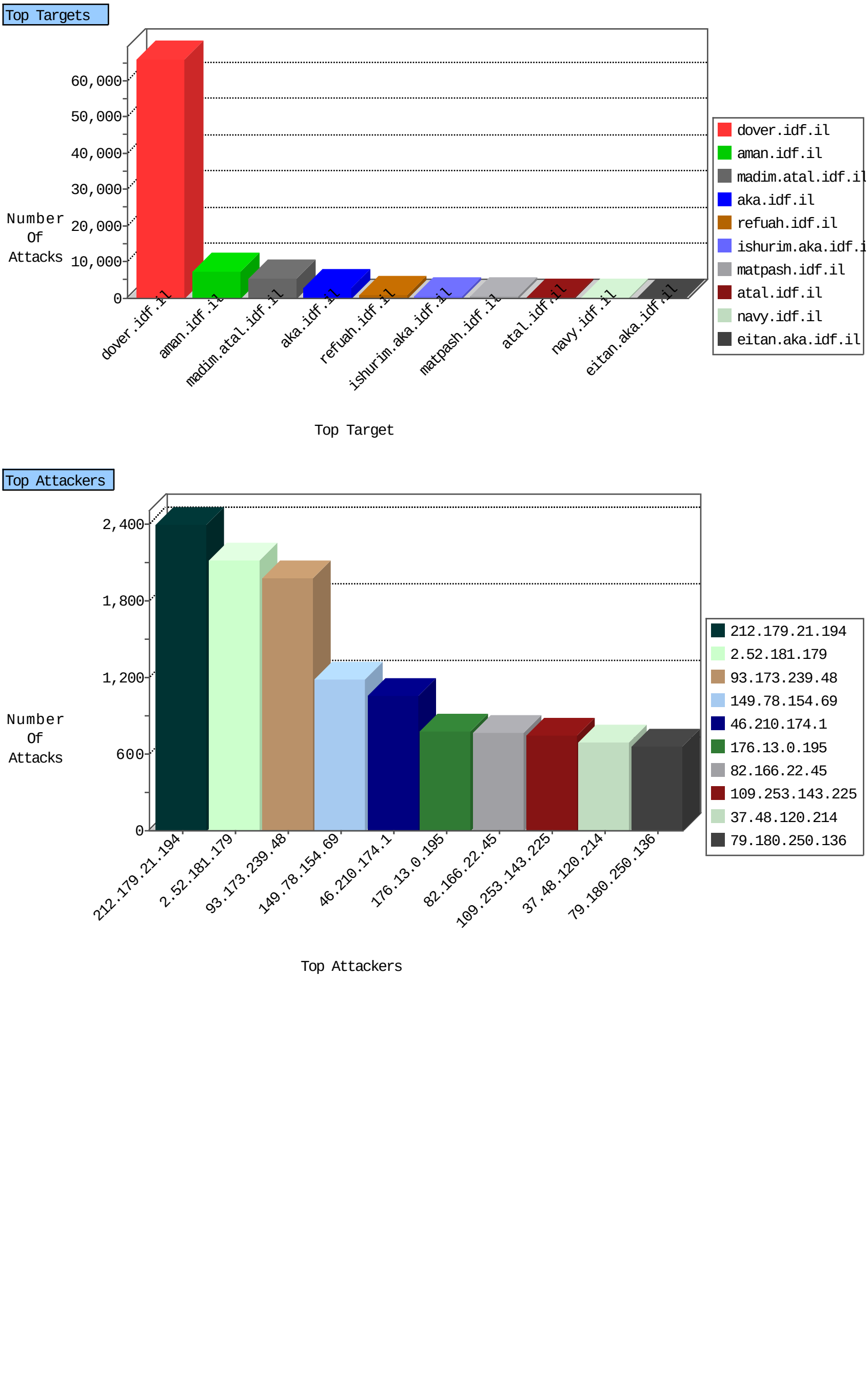
07-19-2015-00:00:08 to 07-20-2015-00:00:08

IDF Under Attack Daily Report



07-19-2015-00:00:08 to 07-20-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	30092
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13568
66.87.65.252	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9494
120.236.165.89	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3954
93.172.161.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2633
84.109.86.175	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1725
79.179.136.163	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1475
94.230.86.141	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	914
31.168.197.116	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	608
84.111.64.178	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	605
46.117.73.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	388
85.65.194.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	352
79.183.115.130	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	298
84.108.132.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	298
87.69.96.31	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	250
176.13.12.242	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	207
95.86.91.115	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
77.125.72.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	185
81.218.46.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	181
217.132.70.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
5.28.187.73	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
79.176.129.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
84.94.163.110	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
109.67.146.185	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
79.182.112.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
84.228.226.99	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
84.111.242.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	157
207.232.1.151	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
213.57.12.89	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
109.65.121.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
79.183.4.158	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	144
84.111.64.178	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	134
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	133
79.181.62.86	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	130
79.176.17.115	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
79.176.173.168	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	128
84.228.33.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
79.183.113.75	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	116
46.116.208.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
199.203.172.65	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
31.168.81.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
62.219.244.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
46.19.85.200	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	101
109.64.139.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	101
79.181.113.18	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
213.57.160.97	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
220.181.108.77	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	87
84.109.17.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
5.29.117.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
89.138.50.70	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83

07-19-2015-00:00:08 to 07-20-2015-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
147.235.236.1	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	25
198.15.178.74	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	22
110.170.188.250	Thailand	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	21
198.15.178.74	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
123.182.150.192	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	7
213.139.53.34	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
46.121.65.193	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
91.228.248.251	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.183.50.153	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.64.249.42	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.179.21.194	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
77.125.151.13	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.29.201.218	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
37.26.146.150	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
31.44.132.202	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
89.139.27.170	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
77.125.241.117	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
117.21.226.103	China	147.237.0.15	kosher-kravi.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	4
212.117.154.106	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
87.69.67.77	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
82.80.22.202	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.98	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.137	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.108.100.251	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.160.188.66	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
41.138.165.205	Nigeria	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
192.116.204.129	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
84.108.139.77	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.186.39.247	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
5.29.112.92	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
41.138.165.205	Nigeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.119	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
82.80.19.242	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.182.8.87	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.114.119.97	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.142.207.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
77.125.12.233	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
87.69.214.57	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
94.159.158.142	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.80.193.236	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.160.173.175	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
79.182.50.72	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
38.99.82.191	United States	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
62.210.251.69	France	147.237.77.216	dover.idf.il	17031: HTTP: GetSimple CMS File Upload	Block	2
188.161.64.17	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
69.23.120.46	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.102.141.249	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.182.183.109	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

07-19-2015-00:00:08 to 07-20-2015-00:00:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.23	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	177
37.8.44.87	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	172
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	80
174.226.128.20	United States	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	47
46.19.85.57	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	6
46.19.85.221	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
82.166.22.45	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	5
94.23.78.16	Portugal	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	3
221.203.3.117	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	3
221.203.3.117	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
66.102.8.178	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
176.12.151.83	Israel	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	2
221.203.3.117	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
176.12.136.37	Israel	147.237.77.170	maarachot.idf.il	GPL SCAN myscan	2
91.121.242.210	France	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.21	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
123.182.150.192	China	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	2
221.203.3.117	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.102	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
176.12.151.83	Israel	147.237.77.216	dover.idf.il	GPL SCAN myscan	2
218.87.111.107	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
45.33.52.199		147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
176.12.136.37	Israel	147.237.77.170	maarachot.idf.il	INDICATOR-SCAN myscan	2
221.203.3.117	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
221.203.3.117	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
66.249.84.146	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
199.203.59.121	Israel	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
91.121.242.209	France	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.111.107	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
79.177.189.50	Israel	147.237.72.156	aman.idf.il	portscan: TCP Distributed Portscan	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.96	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
124.31.206.39	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
95.226.216.150	Italy	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
221.203.3.117	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
84.228.98.191	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

07-19-2015-00:00:08 to 07-20-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2163
2.52.181.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2124
93.173.239.48	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1987
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1181
46.210.174.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1049
82.166.22.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	764
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	694
79.180.250.136	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	655
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	629
141.0.11.156	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	529
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	509
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	485
95.86.121.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	471
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	469
85.250.247.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	441
204.93.58.133	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	438
2.54.131.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	427
79.178.3.192	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	365
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	355
192.115.177.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	345
141.0.14.90	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	342
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	312
46.19.86.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	305
8.37.224.248	Anonymous Proxy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	295
187.141.65.164	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	292
2.54.165.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	290
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	286
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	271
58.170.69.225	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	271
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	270
149.88.97.30	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	266
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	264
37.236.132.98	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	262
46.19.86.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	261
108.35.92.237	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	246
79.177.172.42	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	242
84.228.252.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	237
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	228
87.68.54.41	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	220
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	215
109.64.23.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	212
81.218.172.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	211
84.94.181.18	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	210
141.0.15.14	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	207
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	204
37.26.146.154	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	203
91.228.248.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	195
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	189
212.235.8.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	186
92.40.249.100	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	177

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.13.0.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	777
109.253.143.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.143.225	Block	744
2.54.17.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	369
77.127.199.76	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.127.199.76	Block	323
46.19.85.78	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.78	Block	273
46.117.34.182	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.34.182	Block	271
176.12.138.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	247
176.12.139.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	246
46.19.86.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	223
176.13.5.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	222
176.12.139.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	209
176.13.10.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	192
37.26.148.177	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.177	Block	189
80.246.136.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	165
109.253.146.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	148
176.13.21.33	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.21.33	Block	119
87.69.205.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	117
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	102
176.13.1.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	92
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	82
81.218.193.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
37.26.146.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	80
176.13.5.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.5.225	Block	74
46.19.86.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
176.12.143.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
176.13.23.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
46.19.85.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
2.54.188.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	28
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	27
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	26
37.142.216.49	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	20
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	19
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	19
115.78.235.170	Vietnam	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	18
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	17
5.29.151.24	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.29.151.24	Block	15
218.244.149.208	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.244.149.208	Block	13
31.154.92.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
136.243.36.97	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.36.97	Block	10
82.166.22.36	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9
176.13.9.246	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	9
109.253.149.105	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	8
79.178.191.124	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
85.64.158.194	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	8
176.12.144.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
89.139.61.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
46.121.113.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	8
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7

07-19-2015-00:00:08 to 07-20-2015-00:00:08