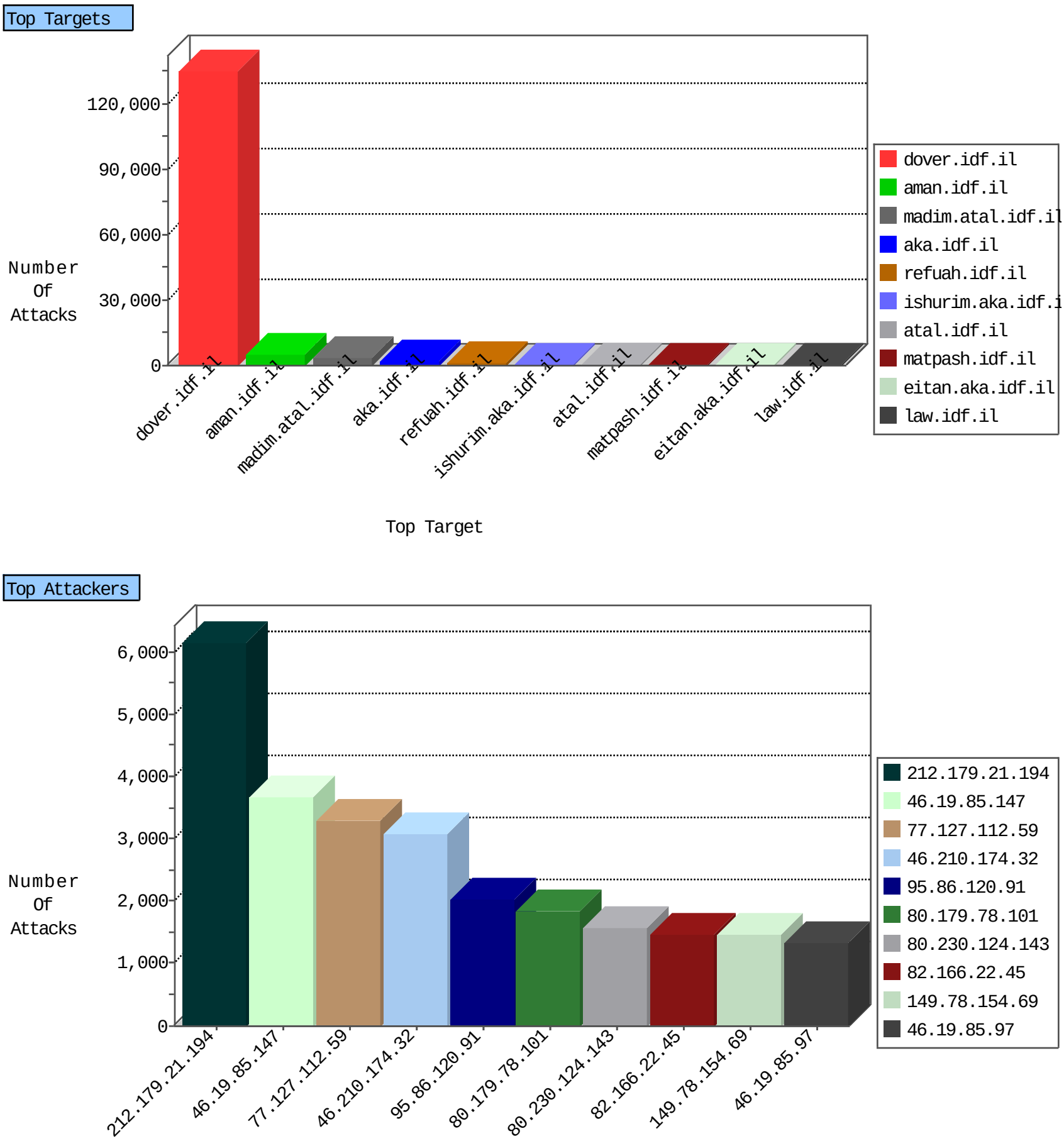
07-20-2015-00:00:08 to 07-21-2015-00:00:08

IDF Under Attack Daily Report



07-20-2015-00:00:08 to 07-21-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.64.102	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3763
46.19.85.183	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2997
79.176.11.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2544
75.108.48.9	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	816
66.249.64.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	652
5.22.129.206	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	537
87.69.193.19	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	427
85.130.246.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	358
79.182.212.160	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	354
79.183.26.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	330
46.120.7.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	289
109.64.50.56	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	281
84.228.141.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	256
46.117.32.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	213
85.250.19.121	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
37.142.143.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	181
84.228.86.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
77.126.90.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
66.249.81.218	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	179
203.26.177.2	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	176
84.109.190.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
79.179.146.189	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
31.154.234.222	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
109.64.177.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
220.181.108.102	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	159
149.78.58.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
79.182.97.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
213.57.186.253	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
84.94.91.68	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
84.109.4.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
84.108.145.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
79.177.158.77	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
109.65.207.224	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
66.102.6.236	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	122
67.187.142.104	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	120
46.116.184.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
37.46.39.148	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	115
185.13.193.185	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	112
31.44.137.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
109.186.128.144	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
109.66.160.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
37.142.126.136	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
85.250.194.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	77
176.13.1.189	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	73
93.172.148.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
213.151.54.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	65

07-20-2015-00:00:08 to 07-21-2015-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.139.53.74	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
85.250.234.190	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
201.130.192.240	Mexico	147.237.76.200	eitan.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
79.178.188.93	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
91.121.11.14	France	147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	6
79.178.22.233	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.139.53.9	Jordan	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.141	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.111.190.226	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
91.121.11.14	France	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	5
85.250.9.118	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
109.67.168.177	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.182.97.29	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
37.26.147.182	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.176.189.195	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
185.13.193.185	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.218	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
82.166.165.228	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.155	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
41.176.208.200	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
99.194.228.212	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.250.125.70	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.64.40.117	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
81.218.151.75	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
31.168.181.69	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
99.21.123.96	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.192	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.143.76.70	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.250.106.5	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.127.26.236	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.176.101.148	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
31.168.136.250	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
81.218.26.138	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.68	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.252	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.64.125.188	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.163	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
94.159.154.67	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
99.237.180.74	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
192.117.33.125	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.26.147.254	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
78.35.188.173	Germany	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.28	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
81.218.156.47	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
192.117.105.110	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
77.125.141.96	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
2.52.0.219	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
95.86.127.41	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.166.119.170	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

07-20-2015-00:00:08 to 07-21-2015-00:00:08

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	128
46.19.85.148	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	48
212.199.57.197	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
82.166.22.45	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	6
74.119.234.98	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	6
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	5
95.110.228.68	Italy	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
221.203.3.117	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	3
66.249.78.172	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
84.108.40.236	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.78.74	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
45.114.11.49		147.237.77.233	atal.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
59.46.193.114	China	147.237.77.212	e.dover.idf.il	GPL SCAN nmap TCP	2
45.114.11.49		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
45.114.11.47		147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
218.24.171.223	China	147.237.77.212	e.dover.idf.il	GPL SCAN nmap TCP	2
85.65.20.191	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
176.12.137.41	Israel	147.237.72.166	aka.idf.il	GPL SCAN myscan	2
218.65.30.107	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.153	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
221.203.3.117	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
198.115.143.10	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
218.65.30.107	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
176.12.137.41	Israel	147.237.72.166	aka.idf.il	INDICATOR-SCAN myscan	2
218.65.30.107	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
118.69.135.178	Vietnam	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
31.168.16.198	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
84.229.29.224	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.203.3.117	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
62.128.48.130	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.32.163	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.172.71.251	Ukraine	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.136.206	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
45.114.11.47		147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.177	Netherlands	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
78.128.92.160	Bulgaria	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 2048	1
218.108.132.58	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
61.55.140.229	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
193.189.116.176	Poland	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
45.114.11.49		147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
199.203.59.121	Israel	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

07-20-2015-00:00:08 to 07-21-2015-00:00:08

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	6027
46.19.85.147	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3678
77.127.112.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3304
46.210.174.32	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3070
95.86.120.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2031
80.179.78.101	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1851
80.230.124.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1584
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1457
82.166.22.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1430
46.19.85.97	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1338
79.178.58.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1280
77.125.162.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1265
192.117.162.62	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1103
37.26.147.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1099
149.88.92.211	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1068
95.35.35.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1033
84.108.38.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1030
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	954
46.19.86.243	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	953
31.168.168.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	896
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	851
2.54.14.73	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	847
46.116.99.61	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	835
95.86.126.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	833
31.44.133.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	824
109.65.193.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	789
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	756
109.66.143.32	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	754
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	731
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	722
85.250.247.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	646
84.229.149.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	613
79.181.175.222	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	609
37.60.46.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	577
79.182.216.216	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	554
185.58.201.37		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	530
66.249.64.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	521
212.98.158.35	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	511
46.19.85.9	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	510
46.19.86.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	508
46.19.86.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	502
46.19.85.110	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	494
37.142.64.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	490
2.52.161.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	479
66.249.64.168	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	477
46.19.86.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	461
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	453
46.19.86.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	446
66.249.64.178	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	420
192.115.177.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	417

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.13.1.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	490
46.19.85.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	397
2.54.39.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	268
176.13.3.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	237
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	214
176.13.13.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	183
176.12.148.17	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.148.17	Block	173
93.172.130.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	152
2.54.31.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	143
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	140
2.54.21.77	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.21.77	Block	130
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	126
2.52.33.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	125
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	109
176.12.145.65	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.145.65	Block	105
2.54.3.115	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.3.115	Block	70
176.13.7.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
176.12.140.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
176.12.147.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
80.246.136.66	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.66	Block	55
176.13.7.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
46.19.85.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
77.124.150.216	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	37
37.142.180.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
80.246.136.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
46.19.86.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
95.86.89.73	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.89.73	Block	18
37.142.104.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
84.94.87.159	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	15
37.142.180.244	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.180.244	Block	13
79.179.147.116	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.179.147.116	Block	11
176.13.14.240	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	9
99.21.123.96	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	8
46.117.104.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
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	8
103.245.44.14	India	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	8
46.120.50.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.50.57	Block	8
147.236.38.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
68.180.229.217	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	7
62.233.56.170	France	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 62.233.56.170	Block	6
80.246.136.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
213.151.54.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
193.111.137.94	Germany	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 193.111.137.94	Block	6
176.13.0.154	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.0.154	Block	6
81.183.218.18	Hungary	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
77.124.150.216	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	5
190.200.166.82	Venezuela	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 190.200.166.82	Block	5
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
179.124.28.11	Brazil	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 179.124.28.11	Block	5
176.228.200.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5

07-20-2015-00:00:08 to 07-21-2015-00:00:08