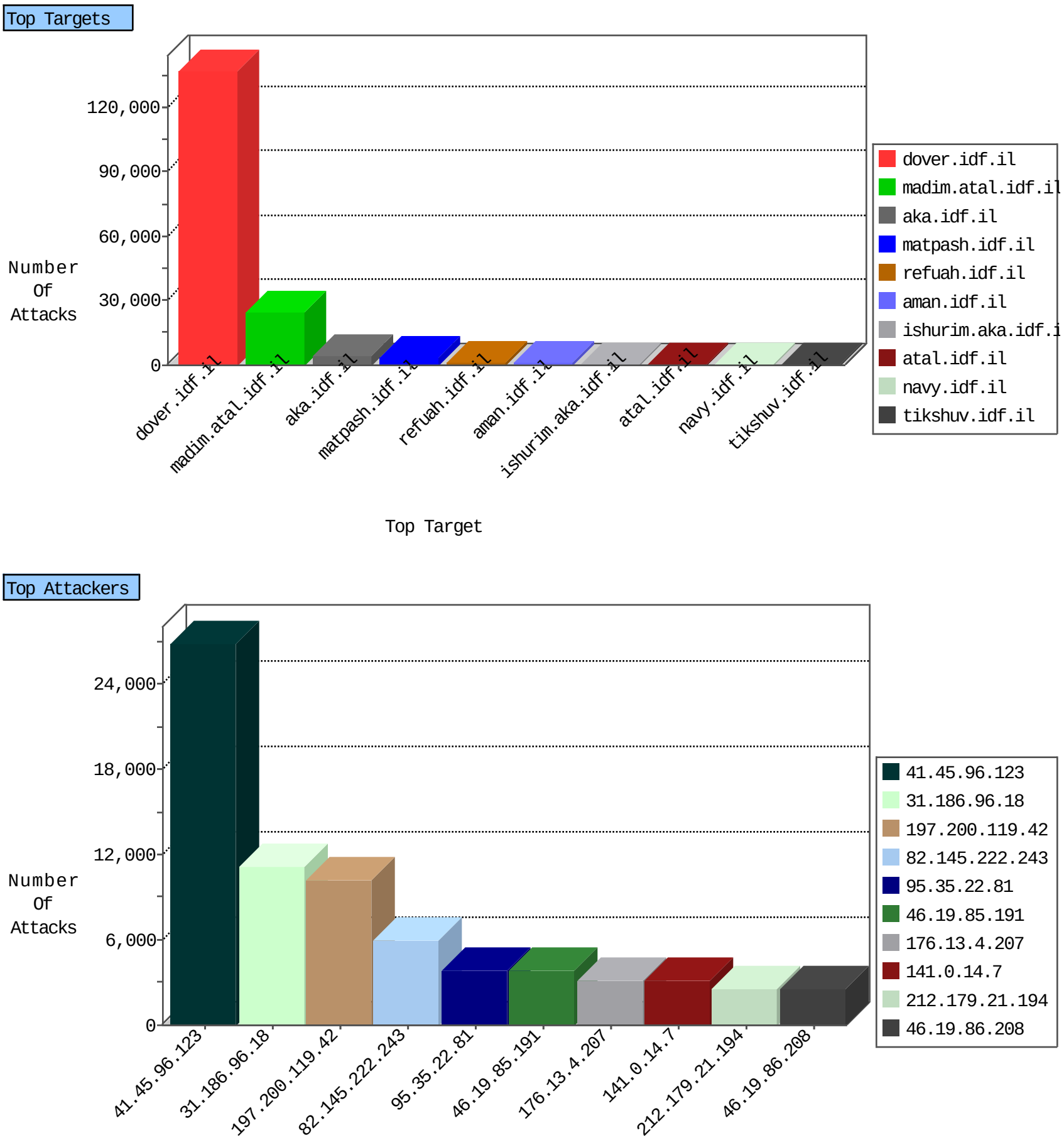
08-25-2015-00:00:06 to 08-26-2015-00:00:06

IDF Under Attack Daily Report



08-25-2015-00:00:06 to 08-26-2015-00:00:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
197.200.74.118	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	42685
197.200.119.42	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	6145
5.42.130.125		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3303
95.35.22.81	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2998
176.13.7.105	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2612
46.117.157.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1550
85.64.217.75	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	623
87.69.144.45	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	617
79.181.59.207	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	542
79.182.183.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	469
89.139.181.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	451
45.33.60.254		147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	448
109.64.62.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	420
109.186.61.64	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	353
46.120.222.223	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	334
79.176.56.1	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	316
79.176.20.166	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	314
84.109.233.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	313
213.57.189.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	267
79.180.52.44	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	257
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	255
79.176.53.118	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	216
109.67.173.30	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	207
84.109.16.75	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	196
89.138.31.68	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	177
87.68.29.83	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
176.13.20.3	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	172
109.66.1.70	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	171
31.154.92.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
77.127.72.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
79.179.96.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
109.67.1.8	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	159
176.228.63.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
185.12.223.146	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	151
37.26.147.220	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	147
2.54.21.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	129
192.116.94.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
109.67.212.15	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
5.102.215.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
85.65.30.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
77.125.0.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
46.116.147.72	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
46.117.127.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
213.57.45.167	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	95
93.172.131.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
46.19.85.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
84.228.200.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
79.181.180.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
109.65.109.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78

08-25-2015-00:00:06 to 08-26-2015-00:00:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.108.242	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	34
84.111.83.145	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	19
212.34.11.81	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	12
212.117.140.170	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
212.143.91.229	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
158.112.84.234	Norway	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
46.19.85.222	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
91.229.61.122	Netherlands	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	7
46.19.85.13	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	7
46.19.85.151	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
46.19.85.13	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
82.80.128.95	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.139.52.58	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
212.143.222.57	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.87	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
69.159.48.165	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
84.108.38.254	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
62.219.54.250	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.152	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
46.19.85.224	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
46.19.85.122	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
31.186.96.18	Russian Federation	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
192.118.11.124	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
46.19.85.144	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
194.114.146.227	Israel	147.237.72.166	aka.idf.il	C1000169: Block - dns poisoning (Clalit)	Permit	3
179.87.190.242	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
208.78.220.140	United States	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
84.108.69.214	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
105.98.53.103	Algeria	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	3
46.19.85.152	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
46.210.130.25	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
109.64.211.180	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
46.19.85.74	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
86.132.157.60	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
109.65.9.92	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.79	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
109.186.185.121	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.142.239.252	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
5.11.45.36	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
85.65.70.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
176.13.6.150	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
79.177.53.190	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
129.130.18.109	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
213.57.164.204	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
31.154.92.123	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
109.64.206.41	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.55	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
77.127.230.167	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
109.66.203.250	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2

08-25-2015-00:00:06 to 08-26-2015-00:00:06

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	67
66.249.67.53	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	12
105.158.178.95	Morocco	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	7
66.249.67.84	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	6
109.66.119.105	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
208.80.155.216	United States	147.237.76.200	eitan.aka.idf.il	Tehila - Perl LWP with fake user agent	4
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
176.13.19.71	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.78.158	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
45.114.11.49		147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	3
199.203.59.121	Israel	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	3
105.158.178.95	Morocco	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	3
199.203.59.121	Israel	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	3
218.65.30.107	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
94.77.157.99	Russian Federation	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.59	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.49		147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
208.80.155.216	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
45.114.11.46		147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
176.228.128.108	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
69.27.63.161	United States	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
79.177.218.224	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
45.114.11.48		147.237.76.39	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	2
85.173.122.122	Russian Federation	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
69.27.63.161	United States	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
61.223.108.145	Taiwan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
83.233.208.235	Sweden	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
123.151.149.222	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
46.116.244.72	Israel	147.237.76.31	nakchal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
37.236.8.178	Iraq	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.26	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.49		147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
37.236.8.178	Iraq	147.237.0.200	m4u.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
45.114.11.48		147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
81.218.133.50	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
94.102.48.193	Netherlands	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
185.32.179.135	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
218.65.30.107	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
197.200.119.42	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	2

08-25-2015-00:00:06 to 08-26-2015-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.45.96.123	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26883
31.186.96.18	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10596
197.200.119.42	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9878
82.145.222.243	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5986
95.35.22.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3889
46.19.85.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3828
141.0.14.7	Europe	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	3098
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2423
2.54.44.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1959
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1790
46.19.85.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1608
95.86.76.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	967
213.151.57.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	936
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	912
95.159.7.197	Syrian Arab Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	782
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	676
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	654
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	638
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	632
212.179.61.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	611
84.111.83.145	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	594
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	527
95.86.72.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	476
31.186.96.18	Russian Federation	147.237.77.216	dover.idf.il		drop	drop	452
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	419
66.249.67.65	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	418
31.44.138.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	416
120.62.19.197	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	414
84.108.158.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	413
92.103.133.165	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	405
79.182.212.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	397
66.249.67.53	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	374
66.249.67.59	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	366
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	358
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	357
37.127.97.10	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	336
46.19.86.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	328
75.107.74.129	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	325
157.55.39.205	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	324
46.19.86.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	305
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	304
213.204.103.26	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	290
37.142.131.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	290
46.19.86.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	254
37.231.76.24	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	237
46.210.157.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	232
212.179.244.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	221
157.55.39.124	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	220

08-25-2015-00:00:06 to 08-26-2015-00:00:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.13.4.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3174
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2487
176.13.10.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2134
176.13.3.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1731
46.19.86.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1682
2.54.147.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1502
37.26.147.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1485
2.54.178.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1440
185.32.179.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1070
85.64.195.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1067
37.142.64.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	990
46.19.86.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	855
2.54.30.51	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.30.51	Block	679
176.12.149.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	575
2.54.49.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	407
176.13.14.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	385
46.19.85.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	325
80.246.136.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	305
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	265
176.13.16.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	250
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	240
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	235
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	225
176.12.148.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	215
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	215
176.13.9.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	215
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.51	Block	180
37.26.146.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	150
37.26.149.138	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.149.138	Block	145
66.249.81.199	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	145
176.13.6.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
79.180.103.124	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.103.124	Block	85
46.19.85.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	70
212.179.21.194	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	65
193.201.224.126	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.201.224.126	Block	60
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	60
192.115.92.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	55
212.179.215.107	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.179.215.107	Block	50
46.19.86.179	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.179	Block	50
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	45
193.37.128.3	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 193.37.128.3	Block	45
79.182.192.146	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.192.146	Block	45
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	35
176.12.146.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
192.114.86.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	35
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	35
66.249.65.99	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
109.66.142.202	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	30

08-25-2015-00:00:06 to 08-26-2015-00:00:06