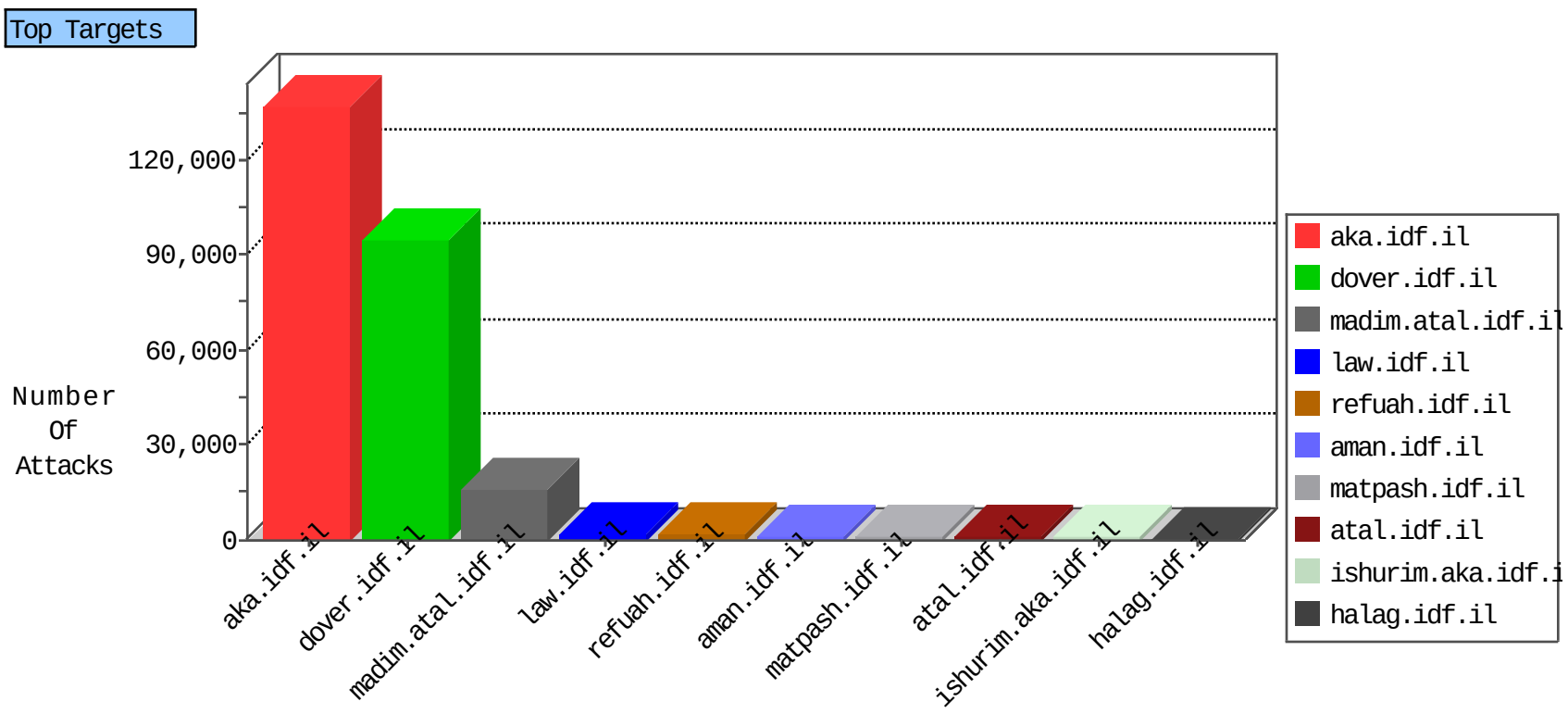
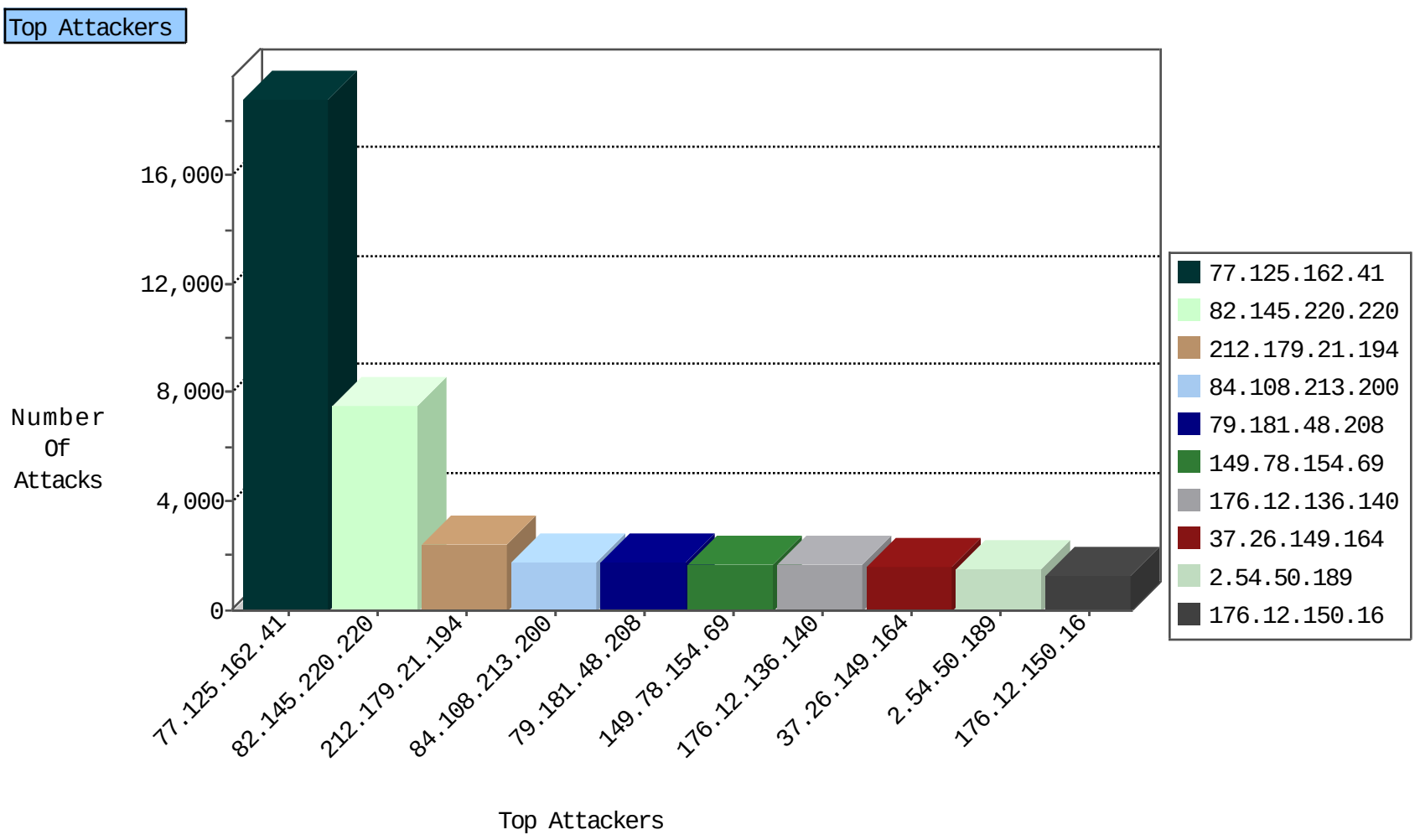
08-09-2015-00:00:08 to 08-10-2015-00:00:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-09-2015-00:00:08 to 08-10-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
176.106.46.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16151
31.13.102.122	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10285
82.166.118.110	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	7456
66.249.64.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4242
68.98.55.68	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2702
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2504
79.182.149.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	787
109.64.200.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	743
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	584
109.64.99.18	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	556
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	533
109.186.100.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	520
79.183.100.120	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	471
87.68.56.80	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	400
46.19.86.249	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	332
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	297
109.64.193.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	285
79.178.188.191	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	281
31.44.136.128	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	277
79.179.179.233	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	277
109.66.105.38	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	269
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	258
79.181.26.180	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	229
46.120.222.228	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	223
95.86.111.216	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	196
84.111.64.178	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
79.176.218.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
109.67.35.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
84.109.4.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
85.250.136.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
79.181.178.11	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
79.179.60.39	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
62.90.219.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
46.120.94.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
85.64.214.89	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	154
85.65.57.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
176.13.20.39	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	143
84.228.150.22	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	137
37.142.64.105	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	126
84.228.46.223	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
85.250.66.209	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	124
76.88.101.212	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	121
31.154.91.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
85.250.211.204	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	114
84.108.219.67	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	111
109.65.134.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
79.178.1.64	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	101
91.231.192.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
134.191.232.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	97
87.69.90.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96

08-09-2015-00:00:08 to 08-10-2015-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.182.149.149	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	65
109.64.99.18	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	41
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	30
45.35.20.195		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	24
194.114.146.227	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
195.191.52.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
45.35.20.195		147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
95.179.34.8	Russian Federation	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	10
109.186.185.78	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
79.182.66.39	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
212.29.194.254	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
194.90.37.80	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.116.134.63	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
197.231.1.160	Mauritania	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.64.36.147	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.57.175.207	Israel	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	6
93.172.117.72	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
84.109.139.130	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.6	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
192.118.48.248	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
213.57.243.61	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.111.178.2	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
212.199.218.246	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.66.48.242	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.176.102.188	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
149.78.253.8	United States	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
195.93.234.9	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.177.215.56	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.61.128.50	Germany	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
5.29.19.139	Israel	147.237.72.166	aka.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	3
84.111.248.23	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.219.126.22	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
80.30.231.54	Spain	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
41.131.117.128	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
82.137.12.108	Romania	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.212	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.65.170.58	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.66.125.159	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
84.228.60.136	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
194.117.2.100	Portugal	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.109.12.37	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.250.47.86	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
122.107.249.146	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.250.64.146	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.125.142.24	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
2.93.99.66	Russian Federation	147.237.76.38	e.e.meitav.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	2
149.78.36.171	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
185.5.223.141	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.57.108.232	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

08-09-2015-00:00:08 to 08-10-2015-00:00:08

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	97
66.249.75.236	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	56
82.166.118.110	Israel	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	10
82.166.118.110	Israel	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	7
82.166.118.110	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	5
211.149.201.209	China	147.237.72.166	aka.idf.il	SERVER-WEBAPP mod-plsql administration access	4
176.12.150.16	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
46.116.94.95	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
192.210.198.132	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	4
220.194.63.2	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.44		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
54.168.76.140	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
45.114.11.49		147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.129	Netherlands	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
132.72.224.217	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
89.248.174.100	Netherlands	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
45.114.11.44		147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
220.194.63.2	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
94.249.44.163	Jordan	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
45.114.11.48		147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.129	Netherlands	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
220.194.63.2	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.129	Netherlands	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
177.85.7.206	Brazil	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
192.249.64.249	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
87.68.244.92	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
93.174.93.129	Netherlands	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
177.190.221.243	Brazil	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
131.108.91.25		147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.129	Netherlands	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
220.194.63.2	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
132.72.138.1	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
89.248.174.100	Netherlands	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
220.194.63.2	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
177.190.221.243	Brazil	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
220.194.63.2	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2

08-09-2015-00:00:08 to 08-10-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
77.125.162.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18857
82.145.220.220	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7502
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1853
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1708
207.46.13.108	United States	147.237.77.74	law.idf.il	SAM rule	drop	drop	1209
109.110.118.146	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	891
68.180.230.29	United States	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	885
66.87.68.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	716
66.249.81.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	700
66.249.81.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	679
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	654
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	646
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	602
188.165.15.209	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	571
79.182.123.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	566
85.65.74.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	523
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	523
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	500
82.145.217.32	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	456
212.179.46.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	441
2.54.182.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	405
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	391
2.52.49.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	376
192.118.64.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	361
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	360
95.86.113.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	358
37.142.253.158	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	353
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	349
84.109.127.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	344
31.44.136.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	344
212.76.97.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	338
190.229.126.235	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	317
72.234.181.211	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	315
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	308
185.4.252.171	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	307
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	297
46.121.64.109	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	291
93.122.177.126	Romania	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	271
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	266
46.19.86.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	265
76.88.101.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
67.68.242.234	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	250
46.19.85.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	231
188.120.151.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	225
98.239.120.115	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	221
85.64.36.147	Israel	147.237.77.234	halag.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	221
82.114.169.114	Yemen	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	217
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	216
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	215
178.252.184.50	Iran, Islamic Republic of	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	214

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.108.213.200	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.108.213.200	Block	1756
79.181.48.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1740
176.12.136.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1707
37.26.149.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1570
2.54.50.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1557
176.12.150.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1313
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.211	Block	1105
176.13.15.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	921
2.54.55.80	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.55.80	Block	879
176.13.11.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	699
85.250.232.104	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.250.232.104	Block	552
176.13.10.154	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.10.154	Block	412
37.60.47.14	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.60.47.14	Block	389
37.26.146.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	387
149.78.50.135	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.50.135	Block	306
176.12.144.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	306
94.230.86.155	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 94.230.86.155	Block	294
176.13.2.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	279
2.54.52.129	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.52.129	Block	261
109.64.165.39	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.165.39	Block	204
79.178.151.200	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.151.200	Block	204
31.154.91.14	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.91.14	Block	201
77.127.26.239	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.127.26.239	Block	201
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	195
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	180
176.12.150.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	171
46.116.146.82	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.116.146.82	Block	168
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	165
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	159
79.182.6.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.6.190	Block	156
2.54.35.221	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.35.221	Block	147
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	144
109.67.1.8	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.1.8	Block	141
176.13.18.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	138
176.13.6.12	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.6.12	Block	138
62.219.138.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/master/vendorscript	Block	138
62.219.138.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/giyusmaster/script	Block	138
62.219.138.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/master/script	Block	138
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	132
85.250.140.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.140.235	Block	131
149.78.197.27	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.197.27	Block	129
5.102.225.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.102.225.40	Block	123
85.64.229.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	111
79.179.19.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.179.19.57	Block	108
37.26.146.247	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.146.247	Block	108
46.117.112.17	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.112.17	Block	102
149.78.20.99	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.20.99	Block	102
79.177.111.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/giyusmaster/script	Block	102
79.177.111.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/master/vendorscript	Block	102
79.177.111.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/master/script	Block	99