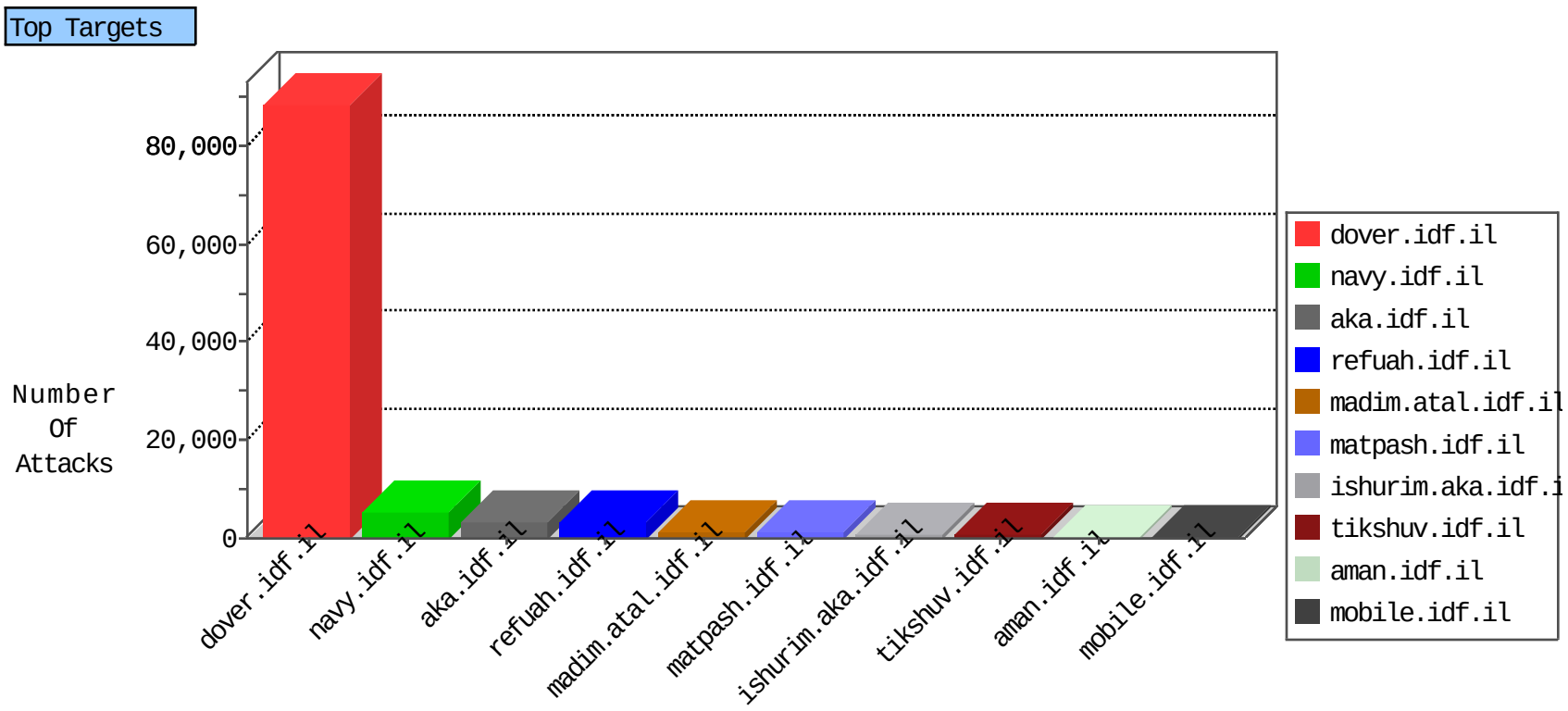
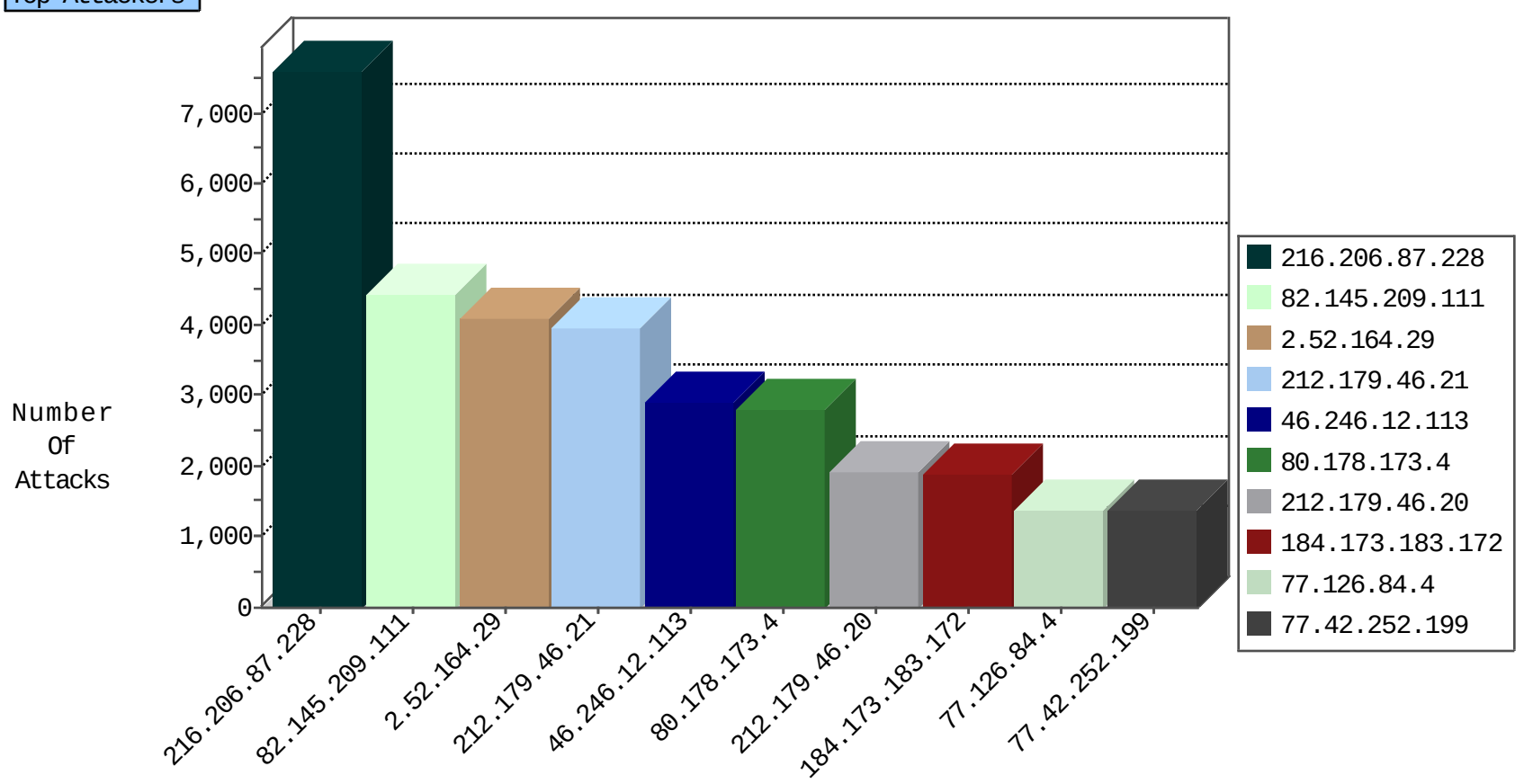
05-07-2015-00:00:06 to 05-08-2015-00:00:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-07-2015-00:00:06 to 05-08-2015-00:00:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8401
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7013
37.231.45.11	Kuwait	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	5416
46.246.12.113	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4107
188.161.79.41	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2917
220.181.108.147	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2540
77.125.99.215	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1661
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1619
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	998
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	853
220.181.108.155	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	828
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	533
220.181.108.118	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	514
84.108.250.96	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	439
84.109.9.152	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	397
79.180.178.147	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	331
176.228.48.33	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	307
147.235.236.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	291
109.253.132.231	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	287
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	282
220.181.108.94	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	262
109.65.142.4	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	247
176.12.146.220	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
77.127.163.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	215
80.12.39.103	France	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
220.181.108.149	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	183
87.68.254.75	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	180
79.181.52.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
213.57.29.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
46.120.80.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
46.121.244.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
220.181.108.84	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	165
66.249.93.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	161
220.181.108.144	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	161
79.182.205.131	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
46.120.73.155	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
5.29.162.232	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	135
212.143.220.82	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
212.179.212.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	123
109.64.188.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
46.19.86.136	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
80.179.184.165	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	103
84.109.9.152	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	102
220.181.108.97	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	97
46.19.86.17	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
79.182.103.60	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86

05-07-2015-00:00:06 to 05-08-2015-00:00:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
216.206.87.228	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	5133
216.206.87.228	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	2002
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	740
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	584
216.206.87.228	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	457
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	281
62.118.222.184	Russian Federation	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	167
184.173.183.172	United States	147.237.76.30	himush.idf.il	DVRep_P-N_40-59	Permit	160
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	128
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	127
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	115
96.44.189.102	United States	147.237.77.216	dover.idf.il	EgovRep_B-N_70-99	Block	24
59.9.253.225	Korea, Republic of	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	21
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	21
119.196.10.1	Korea, Republic of	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
109.226.20.135	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
91.227.164.5	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
213.215.130.101	Italy	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
37.130.227.133	United Kingdom	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	10
197.37.115.59	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
138.134.102.15	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
91.227.165.5	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	7
138.134.102.16	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
138.134.102.16	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	6
85.64.230.176	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	6
80.178.13.141	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	6
31.168.133.168	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
199.203.100.145	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
192.116.94.74	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	6
85.250.24.69	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
46.19.86.128	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	5
62.90.35.105	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
84.109.197.38	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	5
5.29.198.16	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	5

05-07-2015-00:00:06 to 05-08-2015-00:00:06

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	100
188.121.41.145	Netherlands	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	18
37.26.146.180	Israel	147.237.76.42	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
78.108.169.33	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	5
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
46.121.211.116	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
208.80.155.214	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
221.235.189.245	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	3
221.235.189.245	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	3
221.235.189.245	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	3
188.138.9.51	Germany	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	3
221.235.189.245	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.65	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
109.67.159.231	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
183.136.216.3	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
178.19.107.114	Poland	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
77.126.62.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.102.113	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
192.115.83.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.245	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.211	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.111.141.32	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
178.19.107.114	Poland	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
80.246.130.254	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
91.224.132.118	Russian Federation	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.244	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
46.116.219.196	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.121	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
37.142.93.224	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.4	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.244	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
81.218.77.162	Israel	147.237.77.74	law.idf.il	GPL SCAN nmap TCP	2
79.182.203.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.245	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.245	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
37.19.127.166	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.236	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.79	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
109.64.110.100	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

05-07-2015-00:00:06 to 05-08-2015-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.209.111	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4441
2.52.164.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4108
212.179.46.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3958
46.246.12.113	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2849
80.178.173.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2821
212.179.46.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1910
77.126.84.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1384
77.42.252.199	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1377
79.176.200.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1222
2.54.43.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1219
164.138.114.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1209
185.26.182.37	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1120
77.125.88.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1113
82.145.209.182	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	977
37.26.146.176	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	939
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	887
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	874
84.108.176.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	769
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	694
46.19.86.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	675
2.52.130.192	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	591
2.54.163.24	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	479
212.179.21.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	470
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	434
46.116.111.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	421
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	420
212.179.61.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	406
2.52.140.94	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	400
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	380
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	376
2.54.31.0	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	363
108.54.206.238	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	360
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	338
78.108.169.33	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	319
46.121.59.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	314
37.26.148.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	307
95.86.104.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	280
70.39.187.201	Satellite Provider	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	265
70.39.187.193	Satellite Provider	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	263
82.145.220.58	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	256
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	255
164.138.112.97	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	245
197.135.250.31	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	239
2.54.160.112	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	238
62.90.211.107	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	232
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	225
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	219
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	216
213.151.37.67	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	209
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	203

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
31.168.189.107	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 31.168.189.107	Block	579
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	439
2.54.62.0	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.62.0	Block	312
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 78.46.174.55	Block	279
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	279
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	218
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	124
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	122
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	108
176.12.142.22	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.142.22	Block	86
188.121.41.145	Netherlands	147.237.72.166	aka.idf.il	PHP Attempt	Block	47
2.54.151.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
46.116.243.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	24
188.121.41.145	Netherlands	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 188.121.41.145	Block	23
2.52.28.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	22
109.253.135.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	21
46.246.12.113	Sweden	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 46.246.12.113	Block	20
109.186.184.7	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	20
46.246.12.113	Sweden	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	19
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	18
79.182.11.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	17
87.69.85.123	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.69.85.123	Block	16
62.81.85.102	Spain	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.81.85.102	Block	16
207.46.13.3	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.3	Block	15
85.65.11.35	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	15
149.88.6.163	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	13
109.186.12.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
79.181.167.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
157.55.39.64	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.64	Block	11
87.69.35.60	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	11
197.135.250.31	Egypt	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
2.52.28.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	10
93.173.159.227	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	9
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	9
84.94.54.246	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.54.246	Block	9
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.243	Block	8
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
87.79.200.107	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
79.181.101.118	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
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	6
82.80.193.236	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
212.76.96.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	6
212.235.58.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
207.46.13.99	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.99	Block	6
84.94.54.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sip_storage/files/	Block	5

05-07-2015-00:00:06 to 05-08-2015-00:00:06