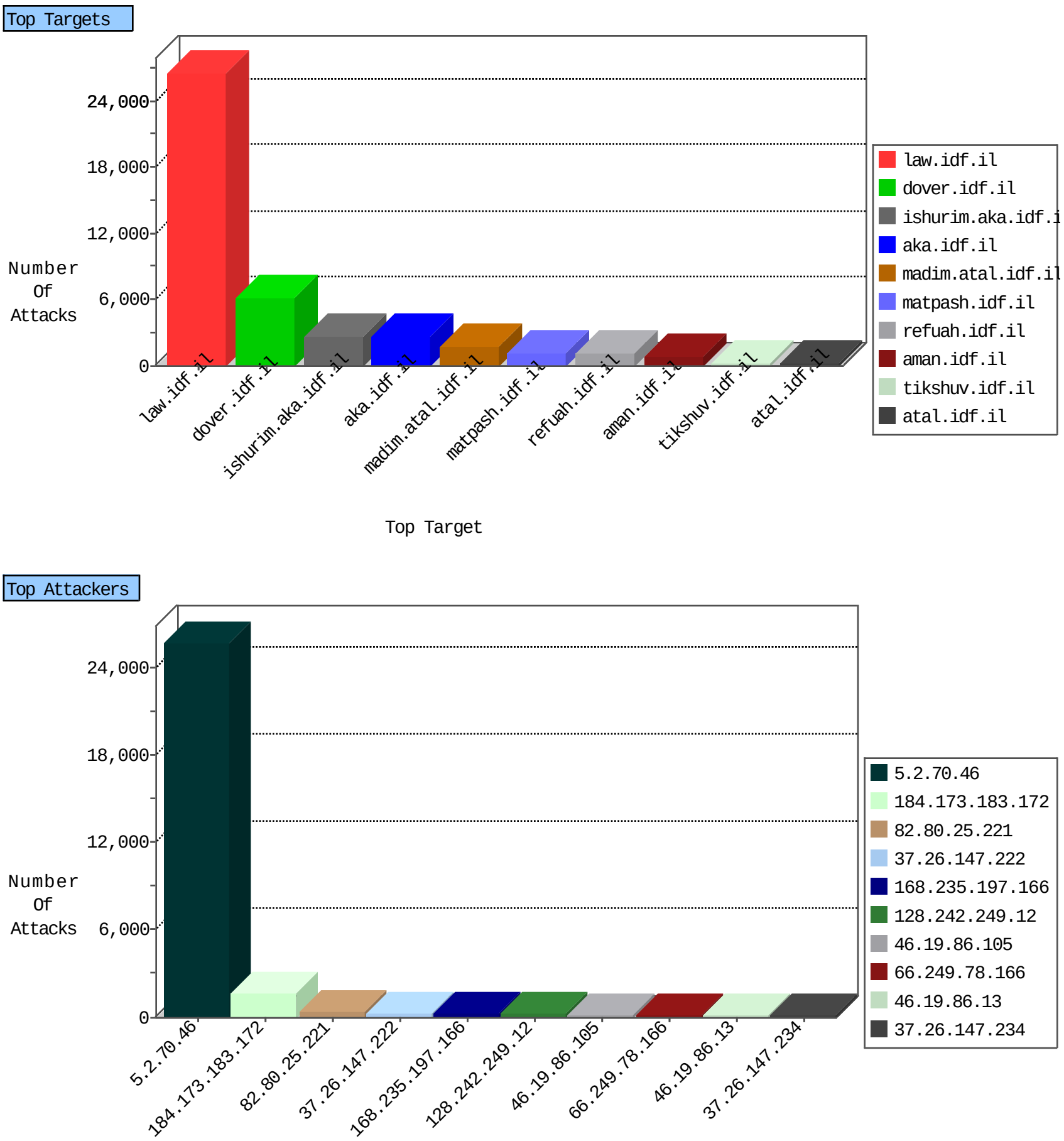
02-18-2015-00:00:04 to 02-19-2015-00:00:04

IDF Under Attack Daily Report

Top Targets



Top Attackers

02-18-2015-00:00:04 to 02-19-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.64.6	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	5869
50.62.135.148	United States	147.237.0.35	akaws.idf.il	TCP Scan (vertical)	drop	5867
66.249.67.116	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4764
66.249.81.183	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4614
66.249.64.132	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4244
66.249.81.206	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4154
66.249.93.154	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4100
66.249.64.124	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4086
66.249.67.108	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3696
66.249.79.157	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3538
66.249.64.14	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3319
66.249.93.187	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3297
66.249.93.195	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2977
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	2756
66.249.64.10	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2385
80.229.223.5	United Kingdom	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2307
66.249.79.50	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2257
66.249.67.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2239
173.11.148.66	United States	147.237.72.167	ishurim.aka.idf.i	TCP handshake violation, first packet not syn	drop	1931
66.249.67.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1917
66.249.79.34	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1826
128.70.154.184	Russian Federation	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1405
73.21.20.105	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1227
31.177.36.114	Netherlands	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	953
95.108.154.251	Russian Federation	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	883
66.249.79.29	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	804
66.249.79.5	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	792
213.244.65.254	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	734
189.100.11.14	Brazil	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	719
66.249.81.228	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	651
66.249.93.158	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	547
188.120.128.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	464
109.65.8.116	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	432
109.66.170.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	419
188.161.3.61	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	388
176.228.136.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	344
89.138.236.88	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	304
46.19.86.89	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	288
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	273
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	234
66.249.67.100	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	205
87.69.228.28	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	187
5.102.216.236	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
79.177.18.115	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
79.177.133.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
109.160.190.230	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
109.186.16.219	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	164
87.68.255.95	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
5.28.188.49	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	161
37.26.147.234	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	159

02-18-2015-00:00:04 to 02-19-2015-00:00:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	587
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	480
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	388
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	275
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	270
46.116.227.155	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	38
109.186.184.53	Israel	147.237.0.15	kosher-kravi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	24
181.68.34.188	Colombia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
62.0.101.97	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
82.80.89.41	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
80.179.16.82	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
159.92.233.88	United Kingdom	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	9
212.34.12.125	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.58.207.103	Turkey	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	6
5.29.106.141	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.34.12.125	Jordan	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.214	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.250.128.43	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
80.246.140.12	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.97	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
190.195.8.141	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	4
68.40.40.176	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.108	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
149.78.233.82	United States	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
84.228.165.50	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.120.194.76	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.66.157.210	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
58.106.160.154	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
5.2.70.46	Nigeria	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	3
68.40.40.176	United States	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
89.31.57.5	Italy	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.181	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.25	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.64.75.23	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	3

02-18-2015-00:00:04 to 02-19-2015-00:00:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	390
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	135
37.9.169.17	Slovakia	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	37
84.111.55.112	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	12
50.62.135.148	United States	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
62.90.202.62	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
109.64.56.134	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
50.62.135.148	United States	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	5
80.246.140.231	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
37.9.169.22	Slovakia	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
84.228.193.150	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
149.78.101.227	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
122.228.207.77	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	3
122.228.207.77	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	3
122.228.207.77	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	3
46.19.85.186	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.238.134.92	Poland	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	2
79.183.29.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.148	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	2
89.248.162.228	Netherlands	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
87.68.17.95	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.248.162.228	Netherlands	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
122.228.207.77	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
2.54.173.82	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.172.121.231	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
77.125.253.38	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
207.46.13.68	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.188.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.161.226	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
5.102.206.216	Israel	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 4096	2
122.228.207.77	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.77	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
89.248.162.228	Netherlands	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.19.85.83	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.79.106	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
79.183.14.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.203.71	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.31.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
109.186.49.90	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.173.191.218	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.178.11.210	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
62.219.62.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.172.30.166	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.67.185.109	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.213.32	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

02-18-2015-00:00:04 to 02-19-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
5.2.70.46	Nigeria	147.237.77.74	law.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	17913
5.2.70.46	Nigeria	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	1938
168.235.197.166		147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	310
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	134
195.212.29.160	Europe	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	114
41.111.41.110	Algeria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	82
82.80.26.105	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	81
131.137.245.209	Canada	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	72
212.179.140.133	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	72
212.116.169.152	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	66
196.217.132.217	Morocco	147.237.77.216	dover.idf.il		drop	drop	66
109.65.8.116	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	53
66.249.79.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
213.8.96.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
109.253.142.103	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
79.179.104.174	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	47
188.122.86.210	Netherlands	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
212.29.249.212	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
37.60.147.30	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	38
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	37
5.22.129.155	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	36
109.253.158.62	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
108.28.18.175	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.139.35	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.148.150	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
212.179.140.133	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	36
168.167.93.245	Botswana	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
87.68.210.31	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
176.12.148.85	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
5.22.129.155	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	34
191.170.94.8	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
109.160.202.8	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	32
213.67.242.13	Sweden	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	31
149.78.249.98	United States	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
176.12.140.185	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.136.3	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.150.155	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.128.192	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.139.60	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
80.178.184.224	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
58.172.33.45	Australia	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
149.88.89.108	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
149.254.180.35	United Kingdom	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	28
91.227.164.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
82.80.84.114	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
109.67.198.84	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
109.253.158.171	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
46.19.86.89	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	26
109.253.159.180	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.2.70.46	Nigeria	147.237.77.74	law.idf.il	Automated Vulnerability Scanning	Block	5956
37.26.147.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	324
46.19.86.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	206
46.19.86.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	172
2.52.33.59	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.33.59	Block	147
176.12.151.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	134
176.12.147.250	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.147.250	Block	114
176.12.137.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
37.26.147.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	80
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.25	Block	67
176.12.148.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
109.186.184.53	Israel	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 109.186.184.53	Block	50
37.9.169.17	Slovakia	147.237.77.176	matpash.idf.il	PHP Attempt	Block	46
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	43
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	41
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.45	Block	39
95.108.158.233	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.108.158.233	Block	39
88.198.180.41	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 88.198.180.41	Block	36
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	36
109.253.147.66	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.147.66	Block	28
132.64.213.95	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	27
217.194.207.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	26
37.9.169.17	Slovakia	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 37.9.169.17	Block	23
46.120.194.76	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	22
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.125	Block	21
37.142.182.152	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	19
65.255.37.160	Satellite Provide	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
212.143.53.57	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	14
157.55.39.121	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.121	Block	14
213.238.175.29	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.238.175.29	Block	13
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.6	Block	13
149.78.235.166	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/undefined	Block	12
109.66.38.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	12
199.168.173.138	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.168.173.138	Block	11
95.108.158.233	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
72.192.216.191	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
95.86.64.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
66.249.79.36	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	10
31.168.142.42	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 31.168.142.42	Block	10
109.66.17.180	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//console/core/doc_mgr/undefined	Block	10
79.181.136.90	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	10
93.172.139.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
79.182.53.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
109.64.129.79	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	9
79.180.97.50	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	8
23.95.138.218	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	8
66.249.79.20	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	8
95.108.158.233	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	8
149.88.92.124	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8

02-18-2015-00:00:04 to 02-19-2015-00:00:04