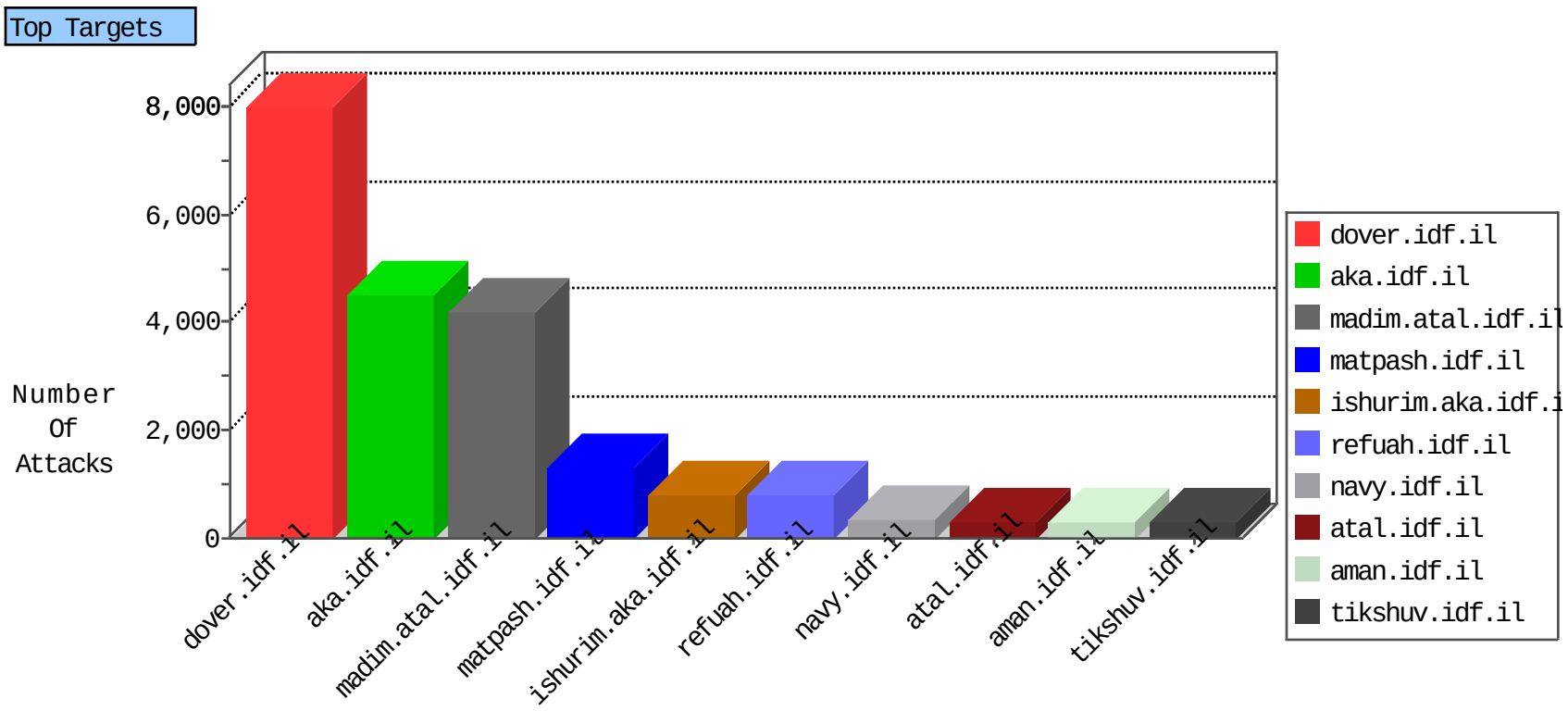
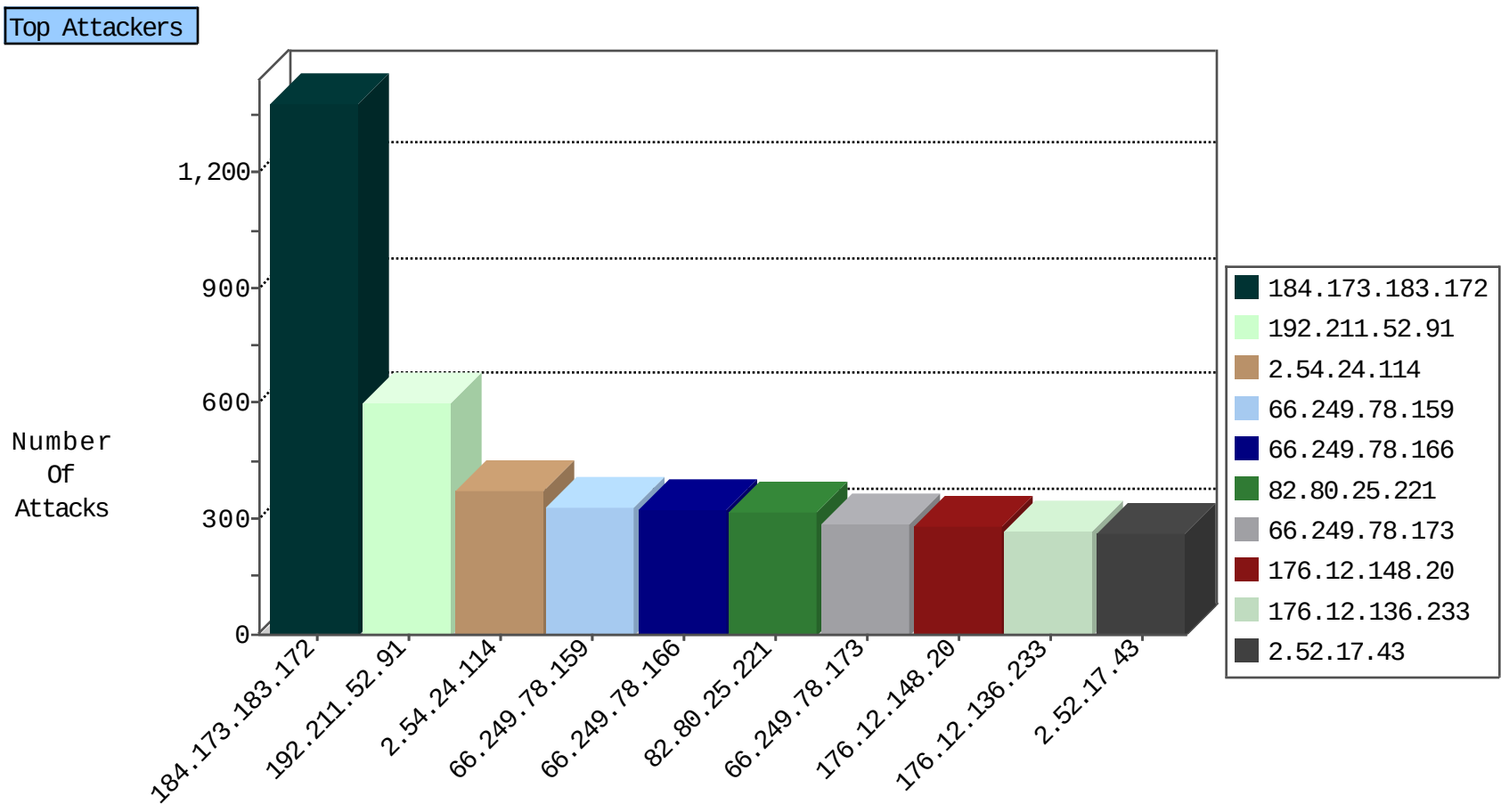
03-30-2015-00:00:05 to 03-31-2015-00:00:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-30-2015-00:00:05 to 03-31-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
199.203.62.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1140
85.250.212.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1033
66.249.67.42	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	957
66.249.78.93	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	949
213.57.13.77	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	893
62.219.227.88	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	546
77.125.215.3	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	532
46.121.82.171	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	477
79.182.165.40	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	373
93.173.171.180	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	349
149.78.219.199	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	342
79.178.52.84	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	307
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	252
93.172.173.138	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	232
85.65.167.135	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	227
212.179.246.19	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	199
46.117.130.47	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	178
89.138.35.84	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	177
2.54.35.63	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	170
95.86.123.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	146
212.235.8.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
37.26.147.156	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	136
37.26.146.163	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	135
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
212.179.46.189	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	124
87.69.203.130	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
84.108.138.39	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
37.142.175.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	104
79.180.121.72	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	90
77.127.198.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
79.181.201.17	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
79.183.127.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
79.183.59.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
79.180.190.164	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
66.249.78.159	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	73
87.68.148.67	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	67
79.182.197.88	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	65
66.249.78.166	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	63
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	61
66.249.78.173	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	57
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	56
207.46.13.16	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	50
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	45
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	44
188.165.15.148	France	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	38
88.198.48.46	Germany	147.237.0.34	tikshuv.idf.il	unblock-sp-traf1	forward	38
157.55.39.6	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	37
207.46.13.112	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	37

03-30-2015-00:00:05 to 03-31-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	828
192.211.52.91	United States	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	600
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	556
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	138
37.59.19.32	France	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	116
199.180.114.150	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	66
212.199.251.235	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
80.179.114.19	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
2.52.13.233	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	17
212.34.12.127	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
94.159.141.68	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
175.44.5.185	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	7
46.19.85.240	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.183.140.144	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	5
149.78.94.147	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	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5
84.229.248.3	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.65.204.49	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.183.34.51	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	4
37.142.144.237	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
149.78.21.180	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
212.34.12.187	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.236.119	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	4
5.28.138.248	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	3
62.0.42.2	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.236.119	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	3
66.240.236.119	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	3
109.226.17.88	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
196.12.162.77	Puerto Rico	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	3
37.144.87.83	Russian Federation	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.236.119	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	3
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	3

03-30-2015-00:00:05 to 03-31-2015-00:00:05

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	321
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	106
2.52.182.78	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	40
85.250.146.221	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	11
2.54.182.48	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	11
208.80.155.147	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	3
115.231.218.147	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.67	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	3
43.255.191.163	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	3
43.255.191.170	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.141	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
190.82.92.3	Chile	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS Wordpress timthumb look-alike domain list RFI	2
37.26.147.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
217.11.61.195	Germany	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
85.64.171.96	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.163	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.163	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
59.41.39.125	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.65	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
82.205.64.177	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.141	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
213.204.127.33	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.163	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
80.178.13.83	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
194.90.37.43	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.75.131	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
134.191.232.69	Israel	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
109.64.124.237	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.163	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.165	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
180.169.108.158	China	147.237.76.200	eitan.aka.idf.il	GPL SCAN nmap TCP	2
43.255.191.163	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.75.110	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
79.182.105.62	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.139.162.218	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.69.175	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.77.162	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
190.82.92.3	Chile	147.237.77.216	dover.idf.il	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt	2
37.26.147.183	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.92	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.66	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.187.69	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.170	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2

03-30-2015-00:00:05 to 03-31-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	230
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	218
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	202
109.65.105.193	Israel	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	148
85.250.146.221	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	142
62.219.161.123	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	122
80.246.133.158	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	109
77.245.172.54	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	78
192.114.105.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	75
188.139.235.252	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	70
85.250.146.221	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	61
37.46.39.91	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	50
94.252.144.35	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	41
189.32.88.90	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
85.130.226.9	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	40
109.253.143.128	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
173.245.115.76	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	37
176.12.147.131	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
59.58.159.217	China	147.237.77.233	atal.idf.il	SAM rule	drop	drop	36
2.52.182.78	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	35
85.65.212.48	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	33
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
74.79.55.236	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.136.156	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.149.76	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
138.134.192.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.143.181	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
81.218.77.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.138.26	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.134.200	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
108.161.241.26	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	30
176.12.144.15	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
108.161.241.27	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	28
173.245.115.77	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	28
108.161.241.22	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	26
85.250.186.142	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	26
80.246.130.131	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	25
92.253.53.231	Jordan	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	25
108.161.241.21	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	25
176.12.146.179	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.65.31.112	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	24
109.253.146.60	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.142.90	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.137.168	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.159.167	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
108.161.241.25	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	23
109.253.159.152	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
2.54.180.81	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.24.114	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.24.114	Block	371
176.12.148.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	275
2.52.17.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	265
176.12.136.233	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.136.233	Block	264
37.26.147.182	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.182	Block	231
176.12.142.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	226
109.253.144.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	216
79.176.182.211	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.176.182.211	Block	206
176.12.142.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	199
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	192
109.253.157.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	184
2.54.3.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	158
46.19.86.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
176.12.151.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	106
109.253.130.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
2.54.10.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	88
109.253.143.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	80
176.12.136.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78
37.26.148.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
109.253.132.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
109.253.142.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
2.54.176.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	69
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
2.52.15.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	57
66.249.81.136	United States	147.237.76.42	refuah.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
66.249.81.140	United States	147.237.76.42	refuah.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
66.249.81.144	United States	147.237.76.42	refuah.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
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	45
109.253.138.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
109.253.130.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
5.29.113.48	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 5.29.113.48	Block	41
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	39
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	37
147.236.38.60	Israel	147.237.77.233	atal.idf.il	Too Many of the Same Response Code (404) in Session from 147.236.38.60	Block	36
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	33
164.138.126.43	Israel	147.237.76.86	navy.idf.il	Too Many of the Same Response Code (404) in Session from 164.138.126.43	Block	31
176.12.145.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
109.253.133.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
109.253.135.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	27
212.179.147.178	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
2.54.141.10	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.141.10	Block	24
109.253.145.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	22
87.69.28.156	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	21
109.253.139.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
83.130.114.158	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 83.130.114.158	Block	16
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
5.29.138.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.138.225	Block	16