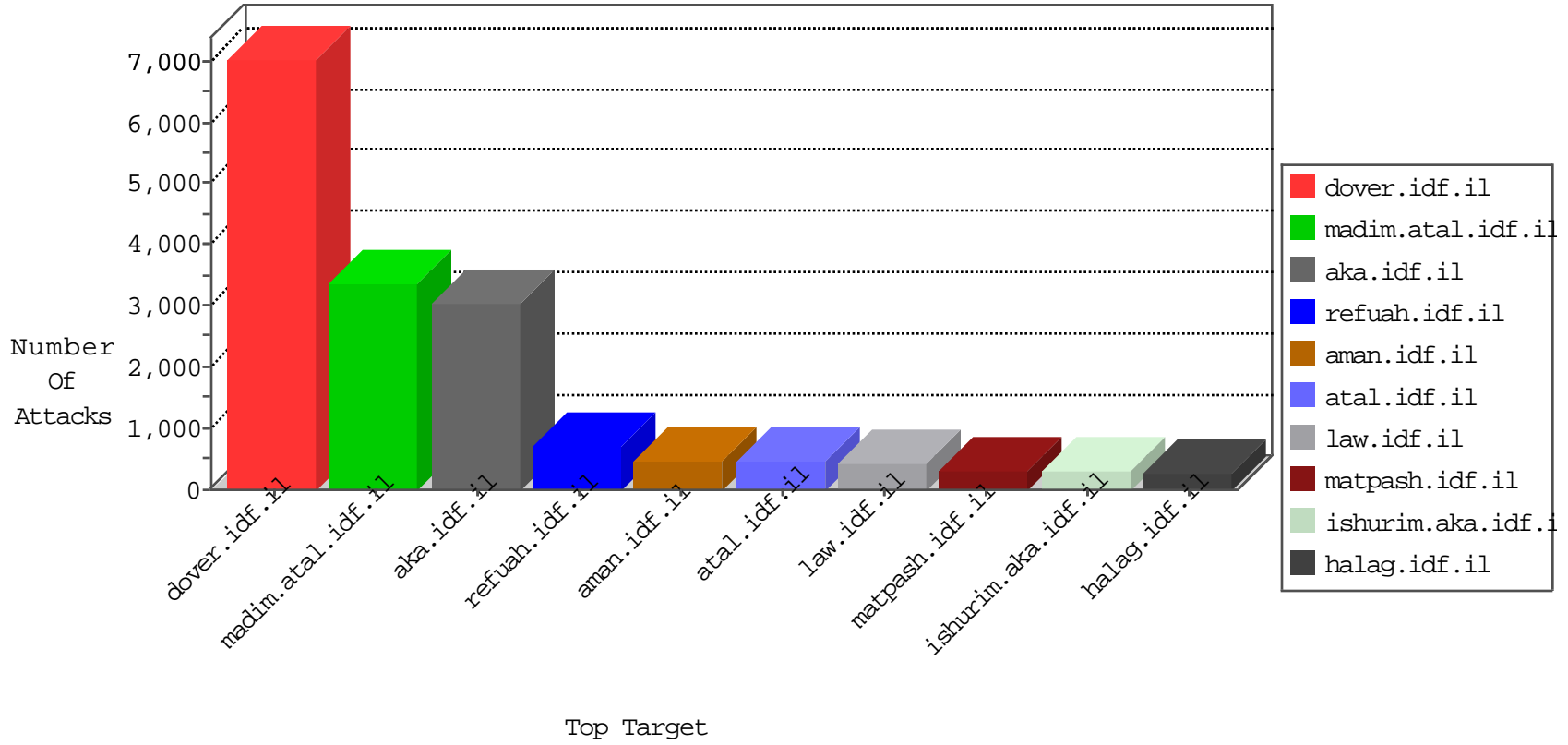


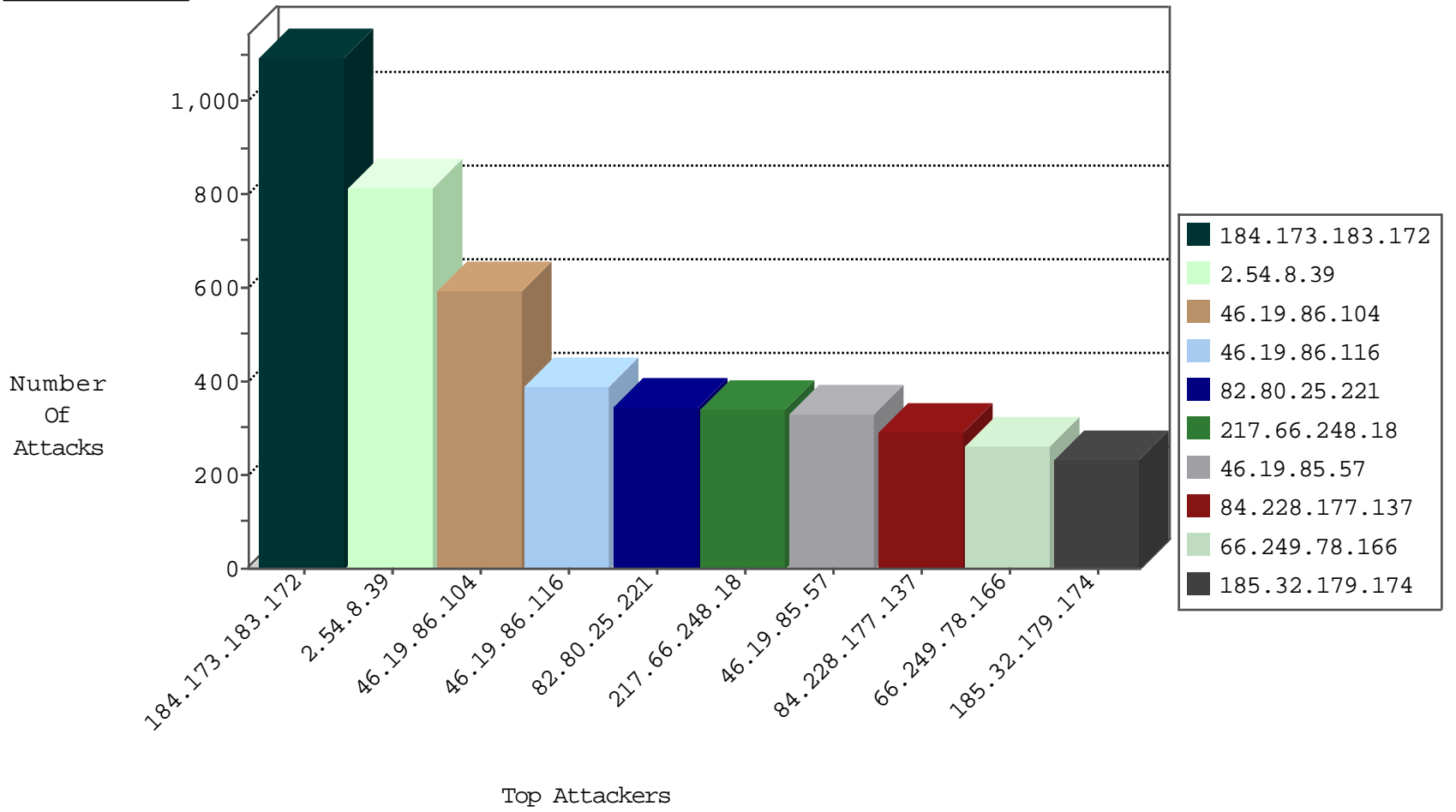
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
217.66.248.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2663
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	691
66.249.78.204	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	588
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	549
46.116.65.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	473
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	428
81.218.51.66	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	358
95.86.125.77	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	320
87.69.168.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	309
85.130.224.14	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	261
109.186.182.161	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	258
85.64.125.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	254
79.176.22.53	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
185.32.178.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	208
79.178.28.111	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	203
46.117.130.163	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
85.250.41.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
79.182.19.251	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
85.250.81.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
213.57.198.66	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
46.120.121.130	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
176.12.138.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
80.246.141.36	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
37.142.175.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
66.249.78.89	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	30
82.102.141.250	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
79.181.127.252	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
46.117.122.150	Israel	147.237.76.42	refuah.idf.il	Anomaly-TCP-SYN-FIN	dest-reset	5
79.176.72.73	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
203.165.161.89	Japan	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	4
95.221.124.99	Russian Federation	147.237.76.42	refuah.idf.il	JIM_Purple_Con_Limit_Http	drop	3
82.102.141.250	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	3
121.80.88.231	Japan	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
79.176.157.205	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.130	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
121.229.220.117	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
202.171.213.183	Hong Kong	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
59.60.104.244	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
183.81.185.137	Cambodia	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
89.248.172.57	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
109.64.170.214	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
79.178.116.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
124.244.32.93	Hong Kong	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	513
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	306
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	276
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	158
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	146
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	64
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	43
2.54.10.111	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
175.44.5.185	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	10
91.212.205.187	France	147.237.77.176	matpash.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	9
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	7
212.34.12.126	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
91.207.4.22	Ukraine	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	6
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	6
85.76.18.206	Finland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
149.88.14.39	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	5
109.65.182.122	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
199.203.63.211	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
89.139.21.138	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.109.18.138	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
203.113.115.18	Thailand	147.237.77.170	maarachot.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
2.71.161.17	Sweden	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	4
46.19.85.214	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
69.197.186.210	United States	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	4
80.179.245.254	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	4
213.57.15.190	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
147.236.31.154	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.227	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.64.42.144	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	3
39.209.132.176	Indonesia	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

## 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	343
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	117
2.52.182.44	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	96
184.168.200.104	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	48
217.66.248.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	25
2.54.176.22	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
109.253.128.138	Israel	147.237.76.30	himshv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	11
203.113.115.18	Thailand	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	8
61.240.144.66	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	3
221.235.188.213	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	3
43.255.191.170	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	3
43.255.191.170	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
149.78.79.107	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.166	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
221.235.188.213	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.166	Japan	147.237.77.234	halag.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
95.86.110.78	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.235.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
115.231.218.147	China	147.237.76.177	ncoore.idf.il	ET SCAN Potential SSH Scan	2
84.228.116.204	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.146	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
79.182.20.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.212	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
77.125.14.167	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.117.160.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.31.144	Israel	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
58.20.54.249	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.141	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
2.54.174.245	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
149.78.238.10	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.94.60.40	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
149.78.123.178	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.170	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.170	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
2.54.32.39	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.166	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.166	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
2.54.13.155	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.212	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
85.64.255.3	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.166	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.212	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.170	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.228.177.137	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	287
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	244
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	196
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	160
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	156
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	156
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	134
194.170.74.98	United Arab Emirates	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	74
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	64
212.25.79.130	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	58
5.28.185.20	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
82.178.234.141	Oman	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	51
213.8.96.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
213.8.50.10	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
109.253.141.187	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
90.174.2.95	Spain	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
85.250.41.143	Israel	147.237.72.156	aman.idf.il	Invalid sequence number	Bad TCP sequence	monitor	40
109.64.42.144	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	37
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.146.234	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.148.58	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.175.97.239	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	35
109.253.139.107	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
176.12.144.147	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
212.25.84.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
109.253.139.50	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
213.57.15.190	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	32
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
192.114.105.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
176.12.149.26	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.130.81	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.156.103	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.134.101	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.133.31	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.140.213	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.146.111	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.141.241	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.160.130.117	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	29
79.178.21.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
109.253.128.138	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	29
201.67.241.199	Brazil	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	28
176.12.141.79	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
179.232.9.183	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
87.68.80.253	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
109.253.128.138	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	alert	27
109.253.149.151	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.128.240	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.143.208	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
197.41.211.79	Egypt	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
2.54.8.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	815
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	594
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	387
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	319
185.32.179.174	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.179.174	Block	232
176.12.150.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	157
176.12.142.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	138
46.19.85.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	128
109.253.143.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	107
80.246.140.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	81
46.19.85.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
176.12.138.228	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.138.228	Block	63
109.253.128.120	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.128.120	Block	63
184.168.200.104	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	47
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
109.253.135.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
37.26.147.213	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.213	Block	24
2.54.61.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
66.249.64.146	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.146	Block	23
184.168.200.104	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 184.168.200.104	Block	23
46.19.85.160	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.160	Block	22
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	21
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	17
109.253.135.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	17
5.29.59.167	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.59.167	Block	16
109.253.140.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	15
66.249.64.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_bottom.asp	Block	14
109.66.10.135	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	14
81.218.48.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	14
203.133.169.208	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.208	Block	13
197.134.127.249	Egypt	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	13
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
87.69.35.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
93.172.163.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
176.12.143.47	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	10
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	10
84.94.32.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
37.26.147.235	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	8
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	8
213.8.76.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	7
209.95.36.61	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/0	Block	7
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_bottom.asp	Block	7
66.249.64.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_bottom.asp	Block	7
212.150.37.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	6
37.26.146.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
95.86.77.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
132.68.114.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	5
106.187.46.34	Japan	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 106.187.46.34	Block	5
109.67.193.244	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.67.193.244	Block	5