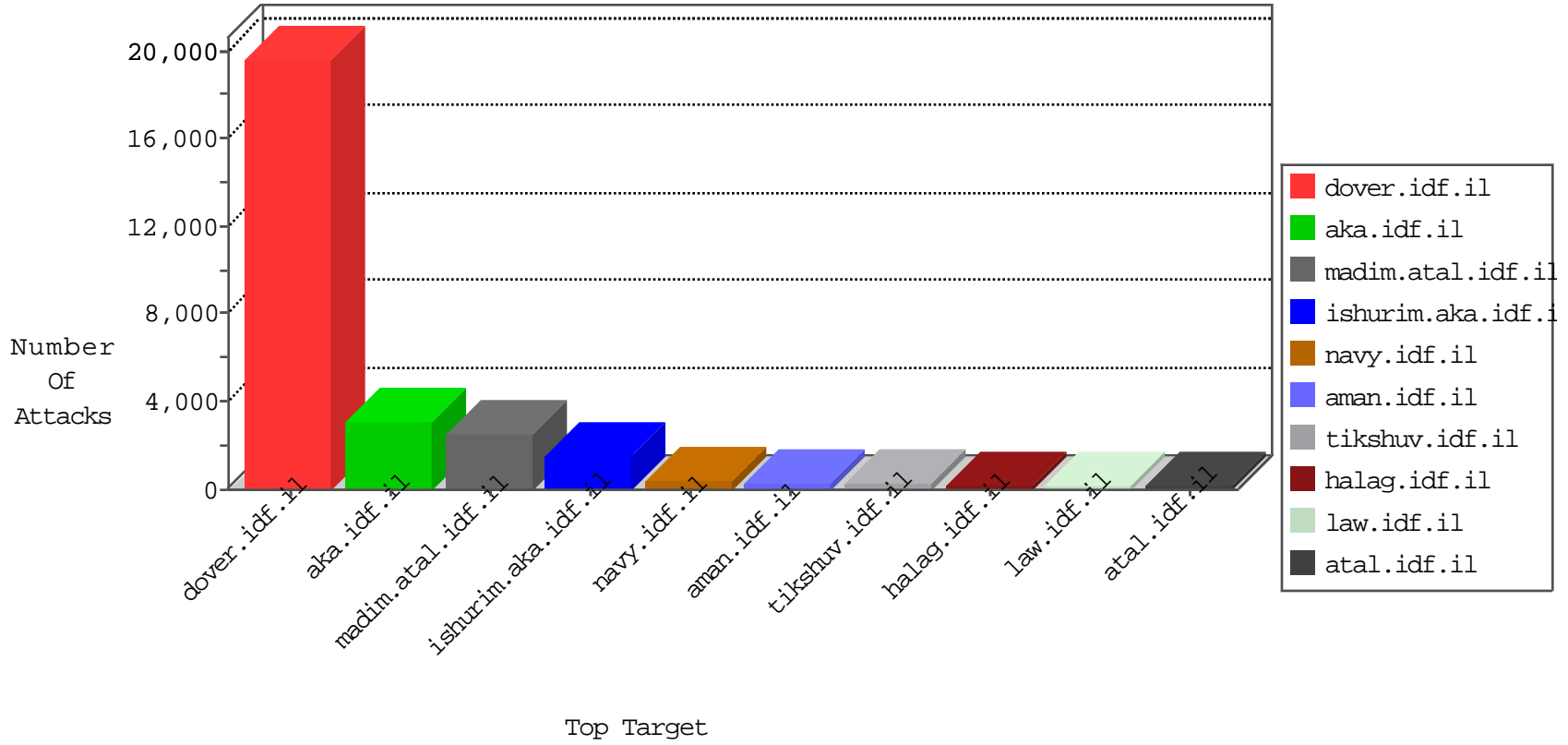


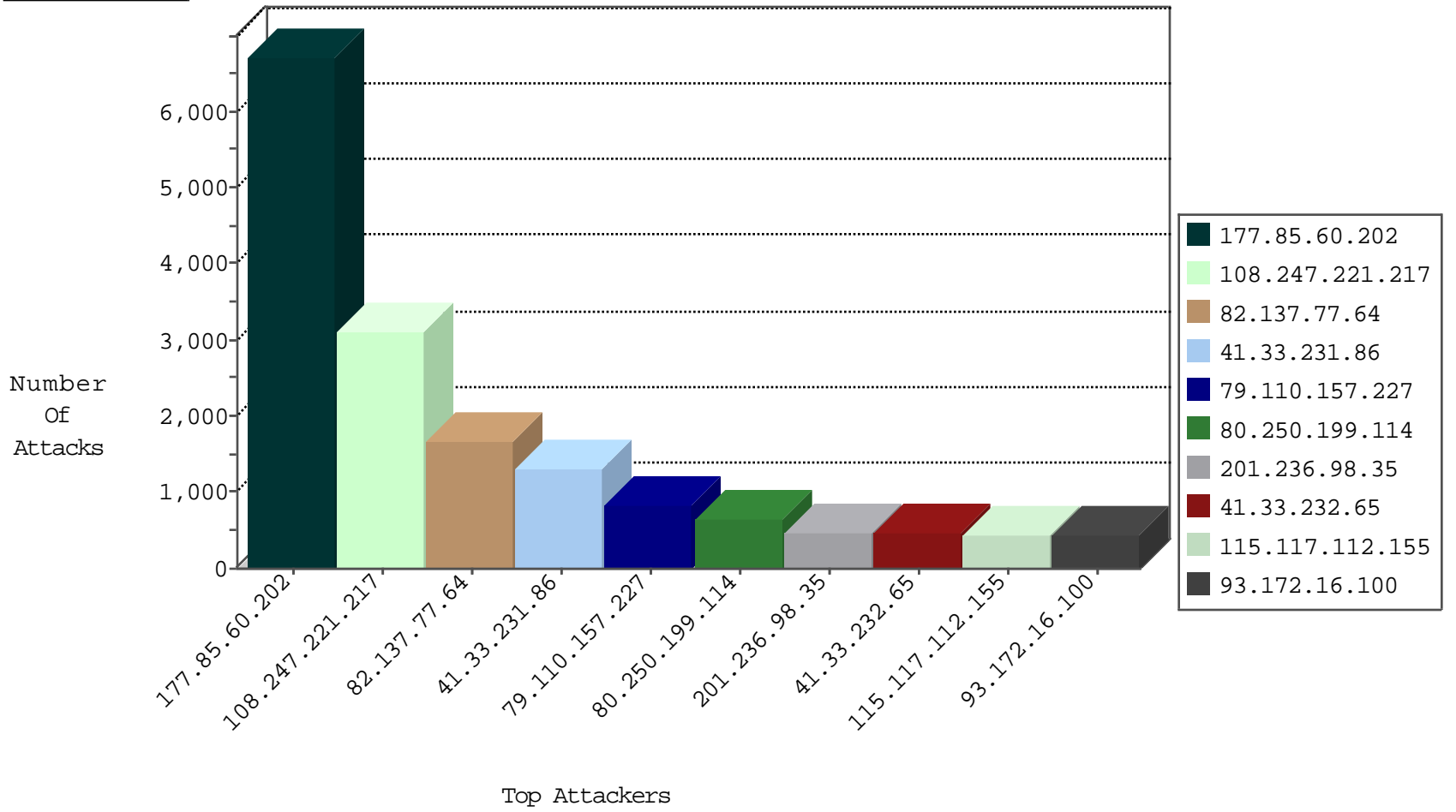
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
213.205.252.64	United Kingdom	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	24120
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	856
201.236.98.35	Chile	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	793
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	736
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Tcp	drop	706
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Tcp	drop	627
201.236.98.35	Chile	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Tcp	drop	488
202.159.228.69	India	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	257
93.172.16.100	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
176.222.247.3	Russian Federation	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	171
202.159.228.69	India	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Tcp	drop	157
176.222.247.3	Russian Federation	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Tcp	drop	110
37.142.241.17	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	drop	104
77.153.96.59	France	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	91
93.172.16.100	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	drop	86
213.57.171.33	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	drop	82
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	drop	74
115.117.112.155	India	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	70
80.246.140.107	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
80.246.137.21	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
93.173.25.78	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	drop	64
195.230.4.43	Bulgaria	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	49
216.155.132.114	United States	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	37
77.153.96.59	France	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Tcp	drop	36
115.117.112.155	India	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Tcp	drop	20
202.216.114.141	Japan	147.237.77.216	dover.idf.il	JIM_Purple_Con_Limit_Http	drop	18
82.102.141.207	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	12
82.145.209.226	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
82.102.141.215	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	8
82.102.141.221	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	6
82.102.141.249	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	4
182.186.125.112	Pakistan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	4
27.3.122.212	Vietnam	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
75.85.21.240	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	4
95.172.79.236	United Kingdom	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
82.102.141.197	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid TCP Flags	drop	3
79.180.121.45	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
124.170.201.187	Australia	147.237.76.30	hinush.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.30	hinush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
84.39.117.99	Europe	147.237.0.34	tikshuv.idf.il	Invalid L4 Header Length	drop	2
204.42.253.2	United States	147.237.76.147	chimuch.aka.idf.il	Block_Ntp_All_Net	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
194.114.146.227	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	36
192.115.248.2	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
218.77.79.43	China	147.237.76.202	e.halag.idf.il	Block_Level_70_100	Block	8
14.99.152.87	India	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
218.77.79.43	China	147.237.76.34	yohalan.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.30	himush.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.31	nakchal.idf.il	Block_Level_70_100	Block	6
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	Block_Level_70_100	Block	6
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	Block_Level_70_100	Block	6
37.75.215.240	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	6
218.77.79.43	China	147.237.76.197	e.himush.idf.il	Block_Level_70_100	Block	6
218.77.79.43	China	147.237.76.148	ggcenter.aka.idf.il	Block_Level_70_100	Block	6
218.77.79.43	China	147.237.77.216	dover.idf.il	Block_Level_70_100	Block	6
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	Block_Level_70_100	Block	6
79.181.29.253	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
218.77.79.43	China	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	Block_Level_70_100	Block	5
198.20.69.98	United States	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	5
66.240.192.138	United States	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	5
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	Block_Level_70_100	Block	4
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	4
218.77.79.43	China	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.72.217	e.idf.il	Block_Level_70_100	Block	4
31.7.57.198	Switzerland	147.237.0.17	m.my-kosher-kravi.idf.il	17056: TLS: OpenSSL Invalid Session Ticket Denial-of-Service Vulnerability (ONLY enable under DoS attack)	Permit	4
85.64.86.244	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	Block_Level_70_100	Block	4
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.76.30	himush.idf.il	Block_Level_70_100	Block	4
85.25.103.50	Germany	147.237.72.156	aman.idf.il	Block_Level_70_100	Block	4
218.77.79.43	China	147.237.8.46	e.chinuch.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	Block_Level_70_100	Block	4
46.151.52.38	Ukraine	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
85.25.43.94	Germany	147.237.76.148	ggcenter.aka.idf.il	Block_Level_70_100	Block	3
71.6.167.142	United States	147.237.72.166	aka.idf.il	Block_Level_70_100	Block	3
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	Block_Level_70_100	Block	3
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	Block_Level_70_100	Block	3
46.116.108.242	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	Block_Level_70_100	Block	3
66.240.192.138	United States	147.237.72.156	aman.idf.il	Block_Level_70_100	Block	3
66.240.192.138	United States	147.237.0.200	m4u.idf.il	Block_Level_70_100	Block	3
78.108.161.226	Lebanon	147.237.77.216	dover.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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	141
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	111
108.247.221.217	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	80
108.247.221.217	United States	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	25
37.75.215.240	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	18
202.159.228.69	India	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	14
201.236.98.35	Chile	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	12
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	10
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	9
115.117.112.155	India	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
176.222.247.3	Russian Federation	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
87.69.205.240	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
201.42.97.49	Brazil	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	4
37.49.224.172	Netherlands	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
80.230.8.179	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
62.152.27.30	Cyprus	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
180.182.76.11	Korea, Republic of	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
213.57.48.21	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
202.216.114.141	Japan	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	2
176.9.50.43	Germany	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
212.179.102.232	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.183.108.200	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.117.112.155	India	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	2
61.240.144.67	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
79.180.136.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
121.125.71.200	Korea, Republic of	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
180.169.108.158	China	147.237.76.39	mobile.meitav.idf.il	GPL SCAN nmap TCP	2
61.240.144.65	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.85.71	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.153.96.59	France	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	2
195.230.4.43	Bulgaria	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
93.174.93.106	Netherlands	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
5.144.57.204	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.134.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.207.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.238.26	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
157.55.39.195	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
82.102.141.254	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
59.67.64.13	China	147.237.72.217	e.idf.il	GPL SCAN nmap TCP	2
112.85.70.6	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
109.64.52.74	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.93.219	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
213.57.45.178	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	SAM rule	drop	drop	4023
108.247.221.217	United States	147.237.77.216	dover.idf.il		drop	drop	2427
177.85.60.202	Brazil	147.237.77.216	dover.idf.il		drop	drop	1614
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1304
79.110.157.227		147.237.77.216	dover.idf.il		drop	drop	821
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	493
82.137.77.64	Bulgaria	147.237.77.216	dover.idf.il		drop	drop	475
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	451
82.137.77.64	Bulgaria	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	435
115.117.112.155	India	147.237.77.216	dover.idf.il		drop	drop	363
62.152.27.30	Cyprus	147.237.77.216	dover.idf.il		drop	drop	350
201.236.98.35	Chile	147.237.77.216	dover.idf.il	SAM rule	drop	drop	344
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	313
82.137.77.64	Bulgaria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		306
82.137.77.64	Bulgaria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	305
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	264
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		257
108.247.221.217	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	202
108.247.221.217	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	195
108.247.221.217	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	160
93.173.8.84	Israel	147.237.77.216	dover.idf.il		drop	drop	150
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		134
79.176.146.23	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	117
79.176.146.23	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence		113
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	110
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	91
85.250.171.32	Israel	147.237.77.216	dover.idf.il		drop	drop	90
105.109.2.89	Algeria	147.237.77.216	dover.idf.il		drop	drop	84
82.137.77.64	Bulgaria	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	77
109.60.137.70	Russian Federation	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	75
82.137.77.64	Bulgaria	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		74
201.236.98.35	Chile	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	63
192.230.140.109	United States	147.237.77.216	dover.idf.il		drop	drop	62
46.19.86.92	Israel	147.237.72.166	aka.idf.il		drop	drop	54
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		51
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	51
216.185.35.36	United States	147.237.77.74	law.idf.il		drop	drop	50
80.246.130.130	Israel	147.237.77.226	www.chamatz.aka.idf. il	Invalid ACK number	Bad TCP sequence	monitor	44
213.8.59.59	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	42
189.212.75.131	Mexico	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	37
192.115.177.203	Israel	147.237.72.167	ishurim.aka.idf.il		drop	drop	36
187.177.26.62	Mexico	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	36
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	35
81.218.183.91	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	32
79.178.187.130	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
109.65.26.64	Israel	147.237.72.166	aka.idf.il		drop	drop	30
115.117.112.155	India	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	29
37.98.218.250	Poland	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	27
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	25
84.108.213.144	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	25

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.172.16.100	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 93.172.16.100	Block	405
84.109.100.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.109.100.27	Block	330
79.181.141.105	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.141.105	Block	295
212.143.71.69	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 212.143.71.69	Block	250
109.253.129.54	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.129.54	Block	225
109.186.122.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
80.246.137.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	188
80.246.137.21	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.137.21	Block	173
207.241.226.113	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	160
185.32.176.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
46.19.86.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
84.108.51.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
87.69.230.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
162.248.48.39	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	62
85.64.103.48	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	54
37.142.207.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	43
82.80.20.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	37
176.12.145.197	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	35
109.64.123.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	34
95.86.67.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	27
79.182.118.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	20
5.29.55.220	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	20
46.116.108.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	20
5.29.113.94	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	19
157.55.39.123	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code Custom Temporary	Block	18
109.253.82.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	16
37.26.148.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	15
68.180.228.167	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 68.180.228.167	Block	15
157.55.39.64	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code Custom Temporary	Block	15
79.177.54.187	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/tzevetavirquestionnaire.aspx	Block	13
66.249.69.35	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/giyus/general.aspx	Block	12
176.12.144.125	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
213.151.48.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
164.138.122.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	11
79.183.32.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	11
157.55.39.242	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code Custom Temporary	Block	11
84.229.48.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	11
46.120.235.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	10
46.19.85.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/tzevetavirquestionnaire.aspx	Block	10
85.250.171.32	Israel	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	10
66.249.69.67	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
164.138.122.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	9
66.249.69.51	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/giyus/general.aspx	Block	9
84.108.51.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	9
31.210.179.113	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
66.249.78.153	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	9
82.80.128.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	8
85.250.61.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8
95.86.82.226	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	8