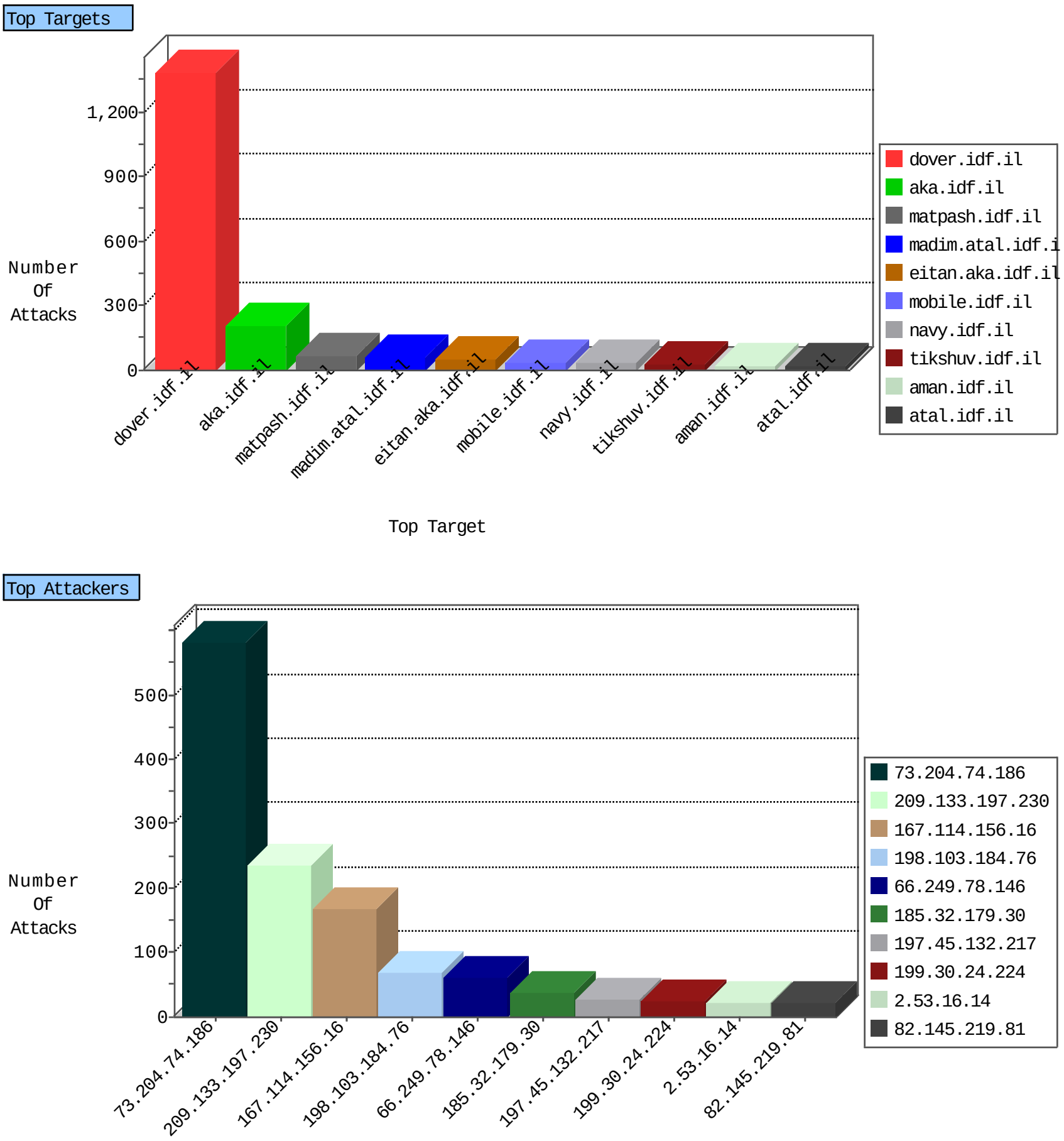
04-25-2016-20:04:03 to 04-25-2016-21:04:03

IDF Under Attack Daily Report



04-25-2016-20:04:03 to 04-25-2016-21:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7046
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	6342
85.65.5.240	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	202
82.145.219.81	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
89.46.102.242	Romania	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
31.148.219.86	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
89.46.102.242	Romania	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
40.78.146.128	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.97.106.162	China	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
45.63.20.231	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
58.221.46.246	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

04-25-2016-20:04:03 to 04-25-2016-21:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.107.127.65	Algeria	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
105.107.127.65	Algeria	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	1

04-25-2016-20:04:03 to 04-25-2016-21:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.160.160.49	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.197	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sA (2)	2
66.102.9.127	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.99	147.237.76.147	Lithuania	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.34	Lithuania	yohalan.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
195.154.54.169	147.237.0.17	France	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.76.199	Lithuania	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.39	Lithuania	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.8.46	Lithuania	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
158.255.5.147	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
96.237.50.37	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.77.61	Ukraine	e.cogat.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

04-25-2016-20:04:03 to 04-25-2016-21:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
73.204.74.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	583
209.133.197.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	184
198.103.184.76	Canada	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	63
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
199.30.24.224	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.53.16.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
129.130.144.219	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
196.134.47.251	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
85.130.207.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.115.95.205	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
149.88.35.111	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
157.55.39.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
76.110.108.115	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
156.170.178.189	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
76.110.108.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
151.41.28.60	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.9.127	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.37.234	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.223.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.43.210.171	Georgia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.156.96	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
50.154.239.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.3.129.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
105.104.184.12	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.18.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
206.210.120.253	Canada	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
37.231.136.15	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
198.103.184.76	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
146.199.101.241	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.131.41	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
156.202.168.165	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
2.53.4.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
163.172.13.244	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 163.172.13.244	Block	6
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.64.23.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
73.168.34.67	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 73.168.34.67	Block	3
66.102.6.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
89.204.155.14	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.160.160.49	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.160.160.49	Block	2
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
178.19.179.58	Poland	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
109.160.191.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
84.109.8.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
5.29.112.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter appDataRequest in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
79.182.40.190	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14886-en/dover.aspx.	Block	1
163.172.13.244	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/facts.asp	Block	1
46.19.86.17	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.182.40.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.175.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
91.200.12.76	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11540-en/dover.aspx/trackback/	Block	1
173.208.177.59	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.19.86.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.160.160.49	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/cityofficers/	Block	1
80.178.1.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
216.21.18.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.154	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
141.8.132.95	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17296-he/dover.aspx.	Block	1
95.90.239.11	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
73.168.34.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
173.208.177.59	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
109.160.191.57	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.130.73	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
68.180.229.180	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
5.29.112.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter appDataRequest in www.aka.idf.il/main/giyus/	None	1
149.88.35.111	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
105.104.184.12	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.181.19.199	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1

04-25-2016-20:04:03 to 04-25-2016-21:04:03