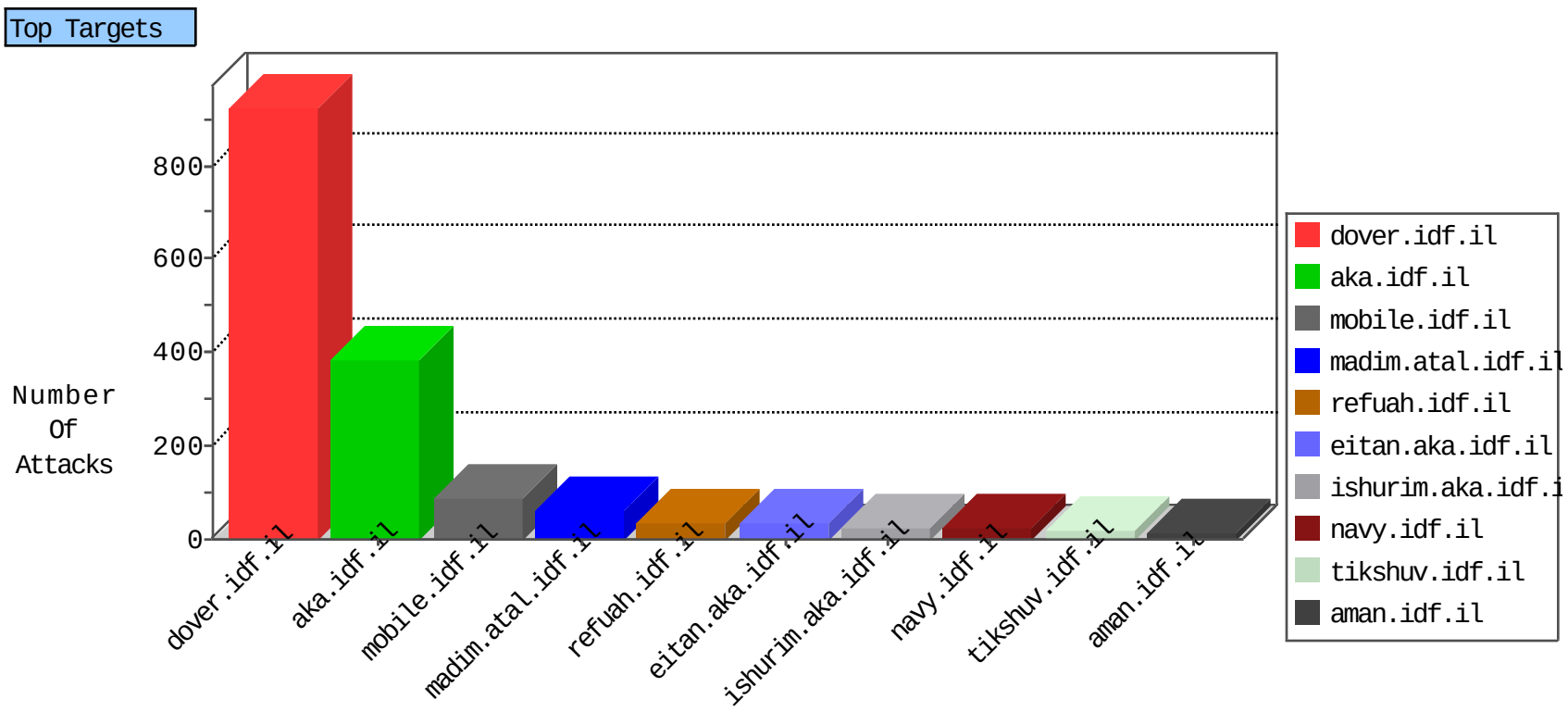
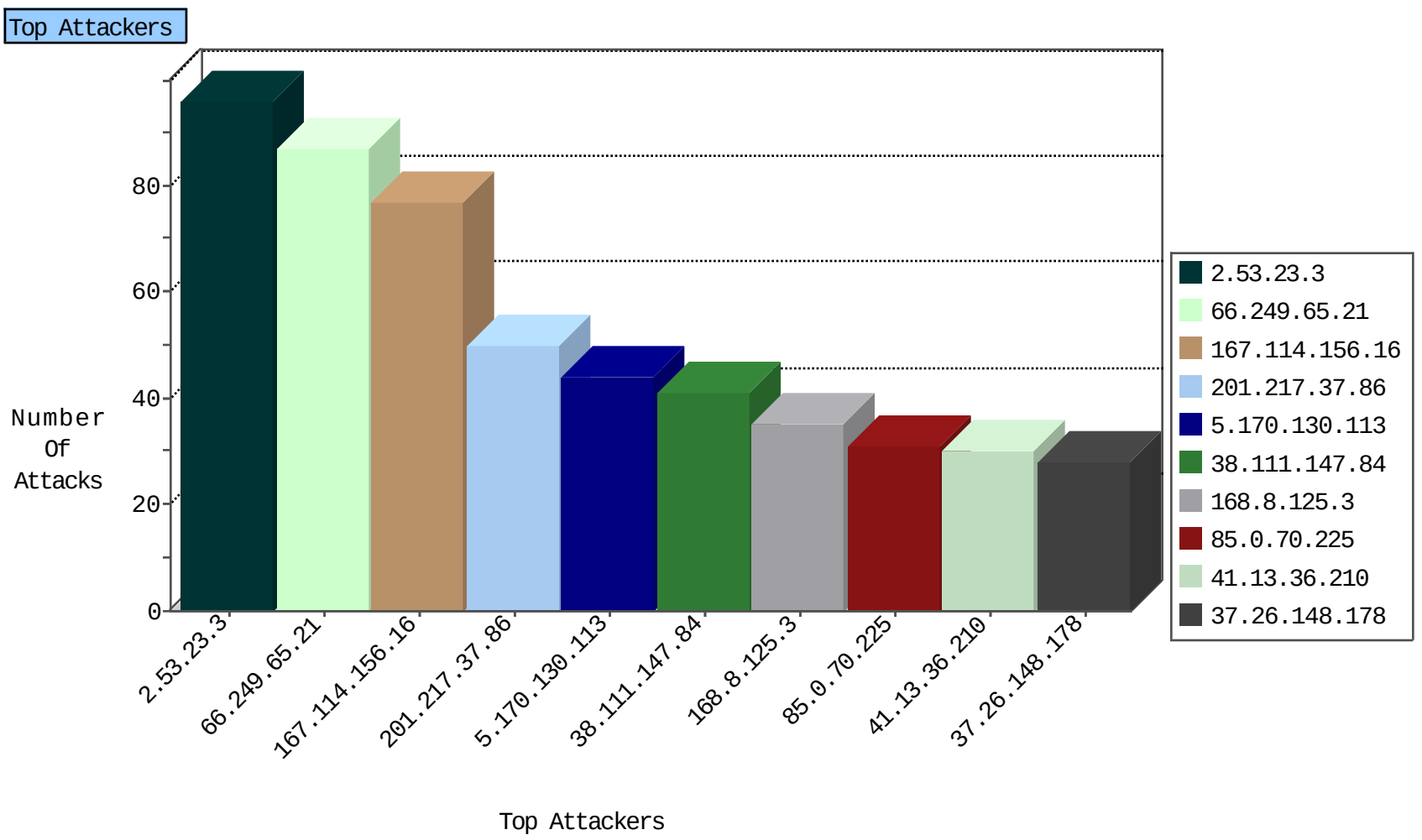
05-03-2016-21:04:05 to 05-03-2016-22:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-21:04:05 to 05-03-2016-22:04:05

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	3368
176.13.9.247	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2728
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	805
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	503
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
141.0.14.218	Europe	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
222.186.50.134	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
141.0.14.218	Europe	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
71.6.216.62	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
107.150.32.59	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
107.150.32.60	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1

05-03-2016-21:04:05 to 05-03-2016-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-21:04:05 to 05-03-2016-22:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.130.143	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
79.177.167.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
63.221.141.195	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
213.8.204.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.62.254.172	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.226.253.118	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
85.65.81.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.212.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.132.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.184	147.237.72.166	Europe	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.116.177.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.62.254.172	147.237.0.33	Canada	idf.il	ET SCAN NMAP -sS window 1024	1
191.181.202.252	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
146.71.100.199	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.78.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.189.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

05-03-2016-21:04:05 to 05-03-2016-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
201.217.37.86	Paraguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
5.170.130.113	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
38.111.147.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
168.8.125.3	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
2.53.23.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
85.0.70.225	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.13.36.210	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
37.26.148.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
2.53.23.3	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	27
46.19.85.93	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
78.162.141.144	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
77.127.133.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
87.71.77.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.53.23.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.183.196.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
85.130.205.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
2.53.23.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.120.126.18	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
64.135.44.66	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
141.0.15.94	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
37.26.146.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.183.110.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.0.30.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.130.223.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.131	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.248.253.133	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.188	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.196.216.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.131	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.180.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
87.71.105.52	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.71.105.52	Block	5
84.108.68.81	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	4
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
202.47.113.226	India	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
77.125.99.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
202.47.113.0	India	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	3
77.127.133.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.37.215	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
216.86.56.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
24.187.198.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.37.119	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 106 cookies	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
96.35.202.58	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.53.22.57	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.105.52	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
203.127.96.201	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.201.222	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/home/default.aspx	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/clientscripts.js	Block	1
176.13.11.3	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
107.150.32.59	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.defences1.com/	Block	1
2.53.22.57	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
220.255.148.146	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
76.123.224.248	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
89.139.158.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.57.138	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
80.86.94.7	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2414.jpg	Block	1
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
62.219.137.5	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 62.219.137.5	Block	1
109.64.180.38	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/1044-he/ishurim.aspx	Block	1
85.64.249.223	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
2.53.23.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
198.209.13.57	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1