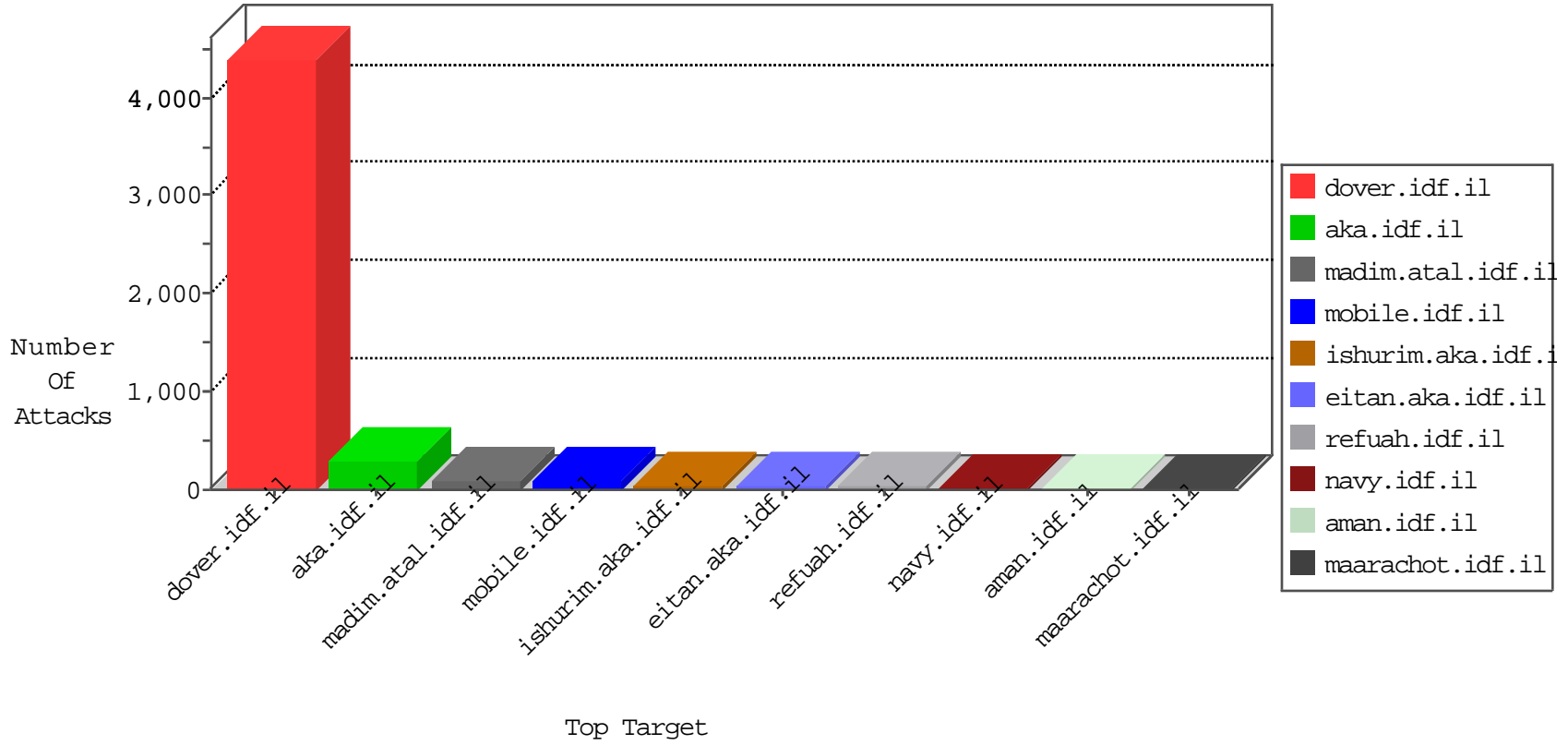


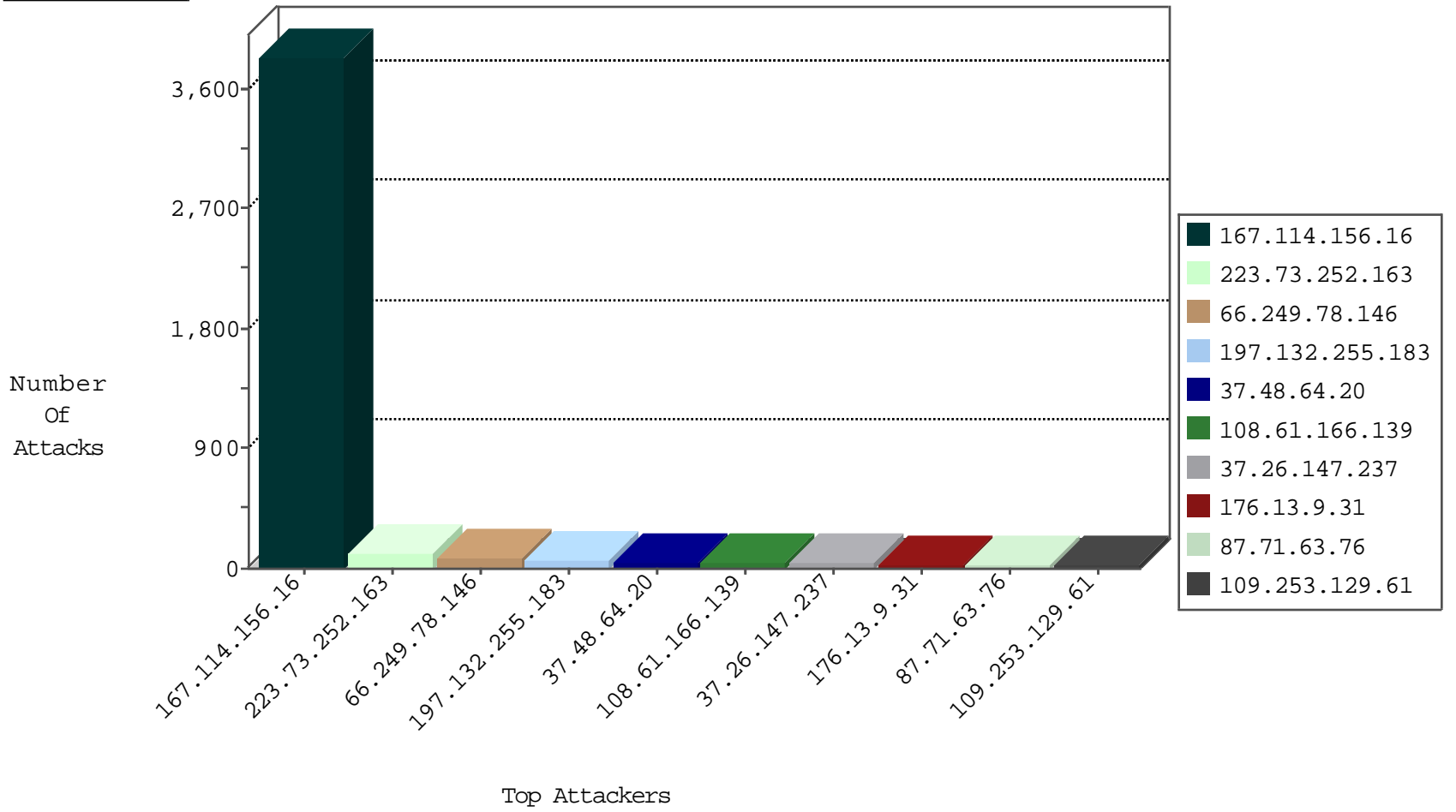
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## 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	7124
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3290
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	580
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
5.196.72.168	France	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
221.1.213.82	China	147.237.8.14	e.orchot.idf.il	Invalid TCP Flags	drop	1
169.54.233.116	United States	147.237.76.34	yochalan.idf.il	Block_Udp_All_Nets	drop	1
169.54.233.116	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.74	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
169.54.233.116	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
223.73.252.163	China	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	3

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
223.73.252.163	147.237.77.216	China	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
54.227.79.235	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
50.19.14.30	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
54.198.161.242	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3426
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
197.132.255.183	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
37.48.64.20	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
108.61.166.139	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
87.71.63.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	25
23.27.45.221	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
176.13.9.31	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.3.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
151.236.162.89	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.253.211.218	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
105.189.112.127	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
87.69.197.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.120.126.17	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.130.174.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.197.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.39.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.44.130.252	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.235.65.236	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.246.139.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.161	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.199	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
97.74.24.187	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.151.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.201.54	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.254.65.30	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.201.54	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.249.89.119	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.9.31	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	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
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.128	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	5
83.244.78.55	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
204.237.2.151	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.196	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
223.73.252.163	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 223.73.252.163	Block	40
37.26.147.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
223.73.252.163	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	27
109.253.129.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
223.73.252.163	China	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 223.73.252.163	Block	11
5.158.236.88	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
5.158.236.88	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.158.236.88	Block	5
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	3
176.13.3.123	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.157.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.197.176	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	2
37.26.149.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.39.183	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.116.66.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.54.102.142	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.237.212.11	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
62.90.255.56	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
223.73.252.163	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fckeditor/editor/filemanager/connectors/php/upload.php	Block	2
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	2
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.161	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SortDir in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
109.66.30.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.90.255.56	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
84.111.234.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/9/	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/enlarge.asp	Block	1
130.185.155.74	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
94.54.101.60	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.75.77.62	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/29/	Block	1
167.114.233.118	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.matpash.idf.il/	Block	1
109.72.215.18	United Kingdom	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/index.php	Block	1
65.55.210.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
141.212.122.129	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /x	Block	1
80.246.139.82	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan*	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/templatecontrols/generic/	Block	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
151.80.31.109	France	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1
62.90.255.56	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 62.90.255.56	Block	1
94.54.102.142	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1