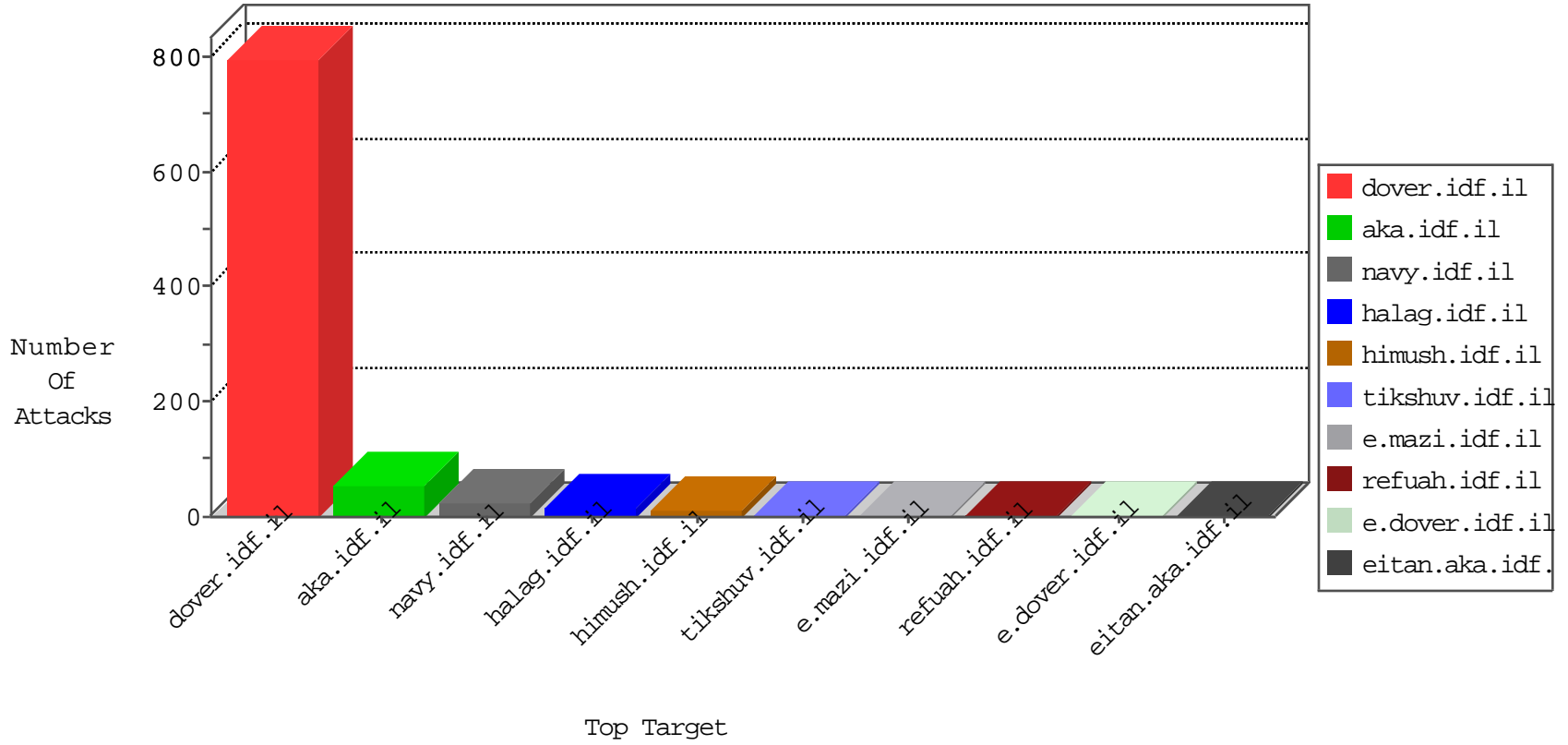


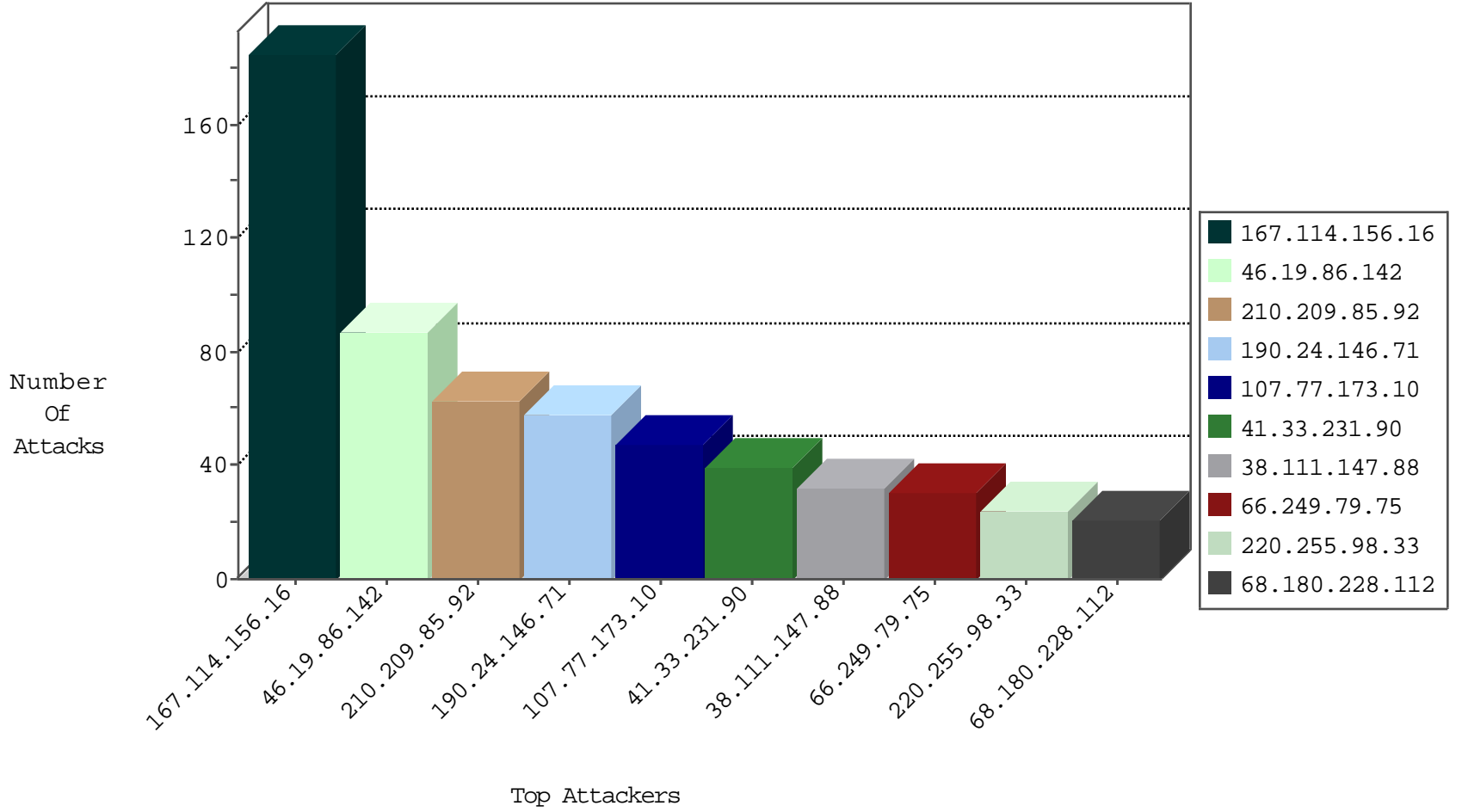
# IDF Under Attack Daily Report



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	6894
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	256
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
210.209.85.92	Hong Kong	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	20
210.209.85.92	Hong Kong	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	8
188.165.15.227	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
62.210.152.89	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
151.80.31.130	Italy	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## 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	5
65.255.43.24	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
178.79.182.42	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
65.255.43.24	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
139.217.27.17	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
112.206.225.86	147.237.77.234	Philippines	halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.60.175	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
85.90.247.26	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
77.109.38.223	147.237.76.176	Ukraine	test.ncoore.idf.il	ET SCAN NMAP -sS window 1024	1
77.109.38.223	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.135	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
65.255.43.24	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
141.105.71.68	147.237.76.177	Russian Federation	ncoore.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
50.204.188.142	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
139.217.27.17	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.60.175	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.60.175	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.108.149.17	147.237.77.61	Israel	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
77.109.38.223	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 1024	1
77.109.38.223	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
107.77.173.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.19.86.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
220.255.98.33	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.142	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
54.215.134.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
40.77.167.0	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.142	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12
199.30.24.119	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.69.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
220.255.103.67	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
208.184.112.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.17	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
104.197.104.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
203.127.96.199	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
67.85.0.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.146.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
96.234.141.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.169.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.6.130	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.142	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
220.255.97.4	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.2.156	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
40.77.167.0	United States	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
94.159.181.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.6.130	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.142	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
219.74.37.10	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.245.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
197.134.124.26	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
173.252.90.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
210.209.85.92	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
74.111.230.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.202	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.79.77	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
210.209.85.92	Hong Kong	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 210.209.85.92	Block	28
176.126.163.232	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
176.126.163.232	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.126.163.232	Block	5
210.209.85.92	Hong Kong	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.124	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/sachar/faq/outerfaq.asp	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
176.126.163.232	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.120.101.155	Spain	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.120.101.155	Block	1
5.29.245.45	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 5.29.245.45 (sigalgs DoS Attack)	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17329.jpg	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
210.209.85.92	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fckeditor/	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
185.3.146.102	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
150.70.97.86	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.120.101.155	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
5.29.245.45	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
210.209.85.92	Hong Kong	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
157.55.39.244	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20475-he/dover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
150.70.173.43	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.64.125.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
210.209.85.92	Hong Kong	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 210.209.85.92	Block	1
109.160.133.219	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 109.160.133.219 (Unknown SSL Session)	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.15	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
150.70.173.43	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
109.201.154.197	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1