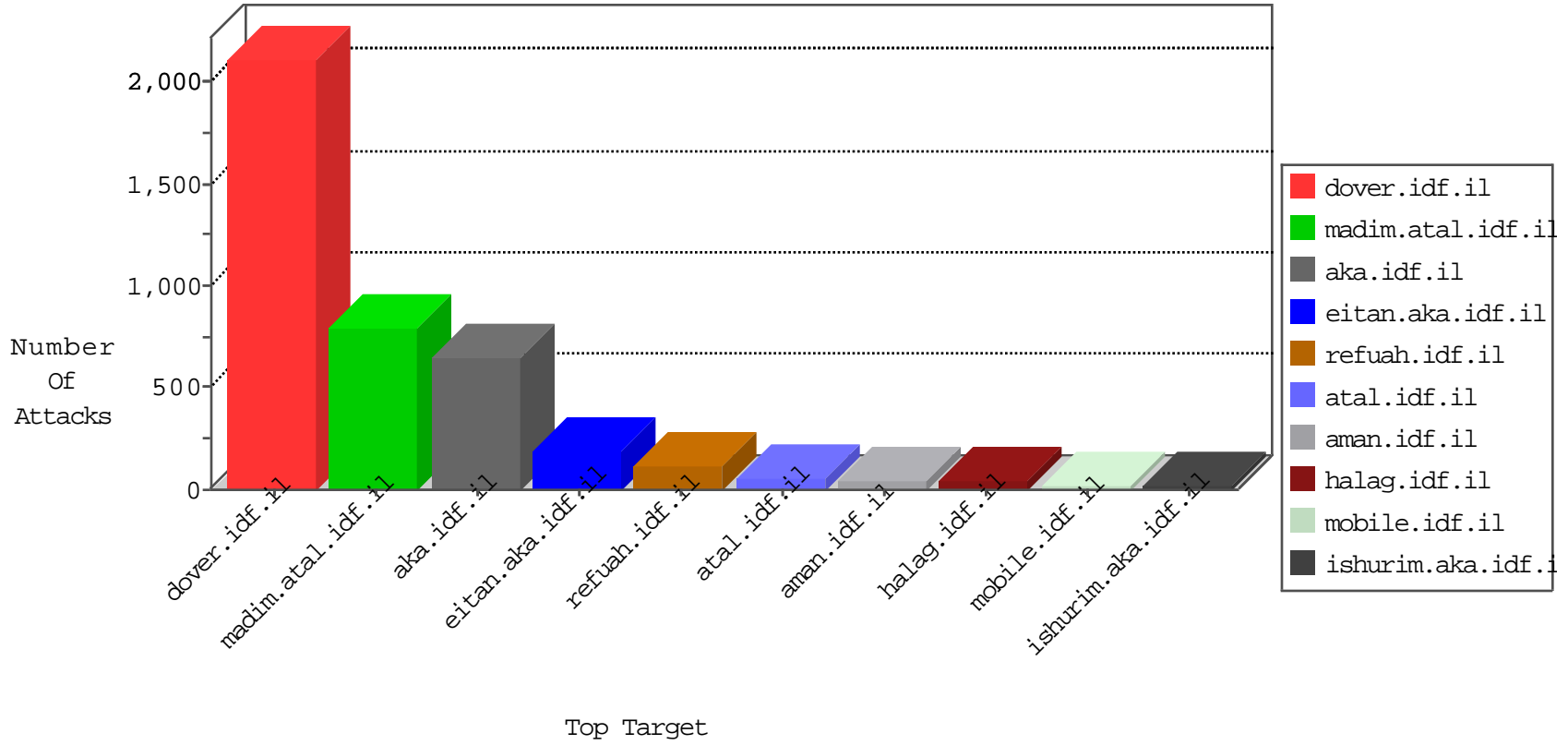


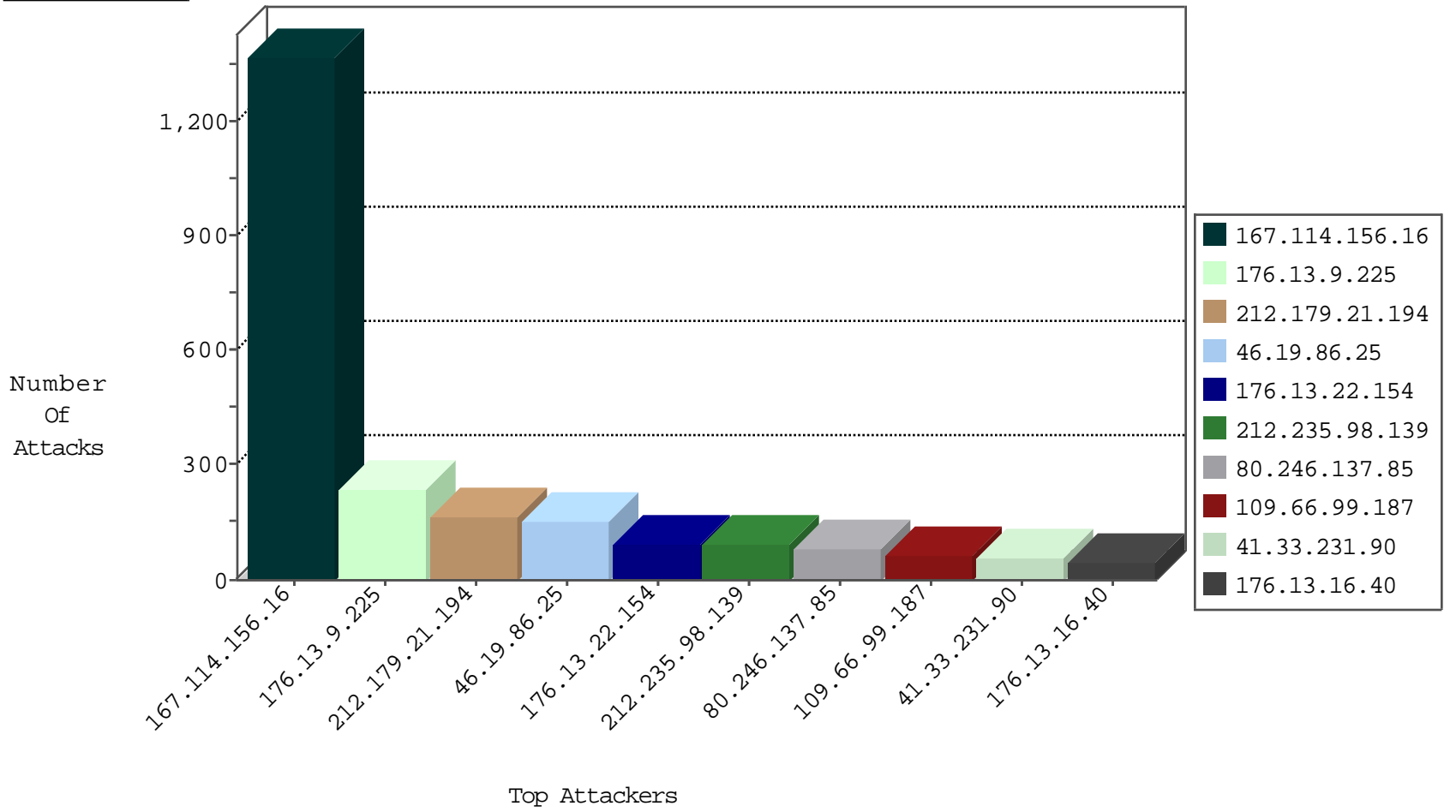
# IDF Under Attack Daily Report



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	3572
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	680
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	363
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	180
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
218.76.143.164	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
192.198.151.45	Europe	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.226.22.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
2.54.17.116	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
62.0.54.152	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
147.236.238.4	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
119.157.1.142	Pakistan	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
151.80.31.130	Italy	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	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	1
176.13.0.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.84.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.10.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.227.170.194	147.237.77.216	Lebanon	dover.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.61.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	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	1065
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	90
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	82
79.179.103.132	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
195.93.246.47	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
76.127.38.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
80.246.130.186	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	21
70.199.69.182	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
84.228.29.115	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
37.26.146.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
217.55.175.67	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.54.164.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
207.46.13.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.116	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
104.131.246.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
131.253.25.228	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.138.238	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.107	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	10
83.130.102.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.99.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.54.164.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.54.164.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
157.55.39.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.164.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
84.228.29.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.154.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.135	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
31.168.165.94	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
183.79.219.165	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.79.79	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.226.51.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
183.79.219.165	Japan	147.237.77.216	dover.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
176.13.9.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
176.13.9.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
176.13.22.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	80
80.246.137.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
109.66.99.187	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.66.99.187	Block	55
176.13.16.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.54.46.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
80.246.136.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
37.26.147.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
2.54.1.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
62.90.35.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	15
81.218.251.252	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.80.196.44	Block	11
176.13.9.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	10
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	9
62.0.54.152	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 62.0.54.152	Block	6
109.186.62.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	5
2.54.139.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.246.137.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
85.250.6.255	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	4
80.246.136.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
62.219.99.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.151.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
209.88.183.121	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
176.13.16.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
176.13.8.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.16.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.19.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.195.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
109.186.62.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
2.52.171.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
209.88.183.121	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
176.13.7.242	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
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	2
87.69.211.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
85.130.223.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.6.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
62.90.202.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
176.12.149.73	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
2.54.182.19	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
80.246.140.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/qiyus/login.aspx	None	1
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1