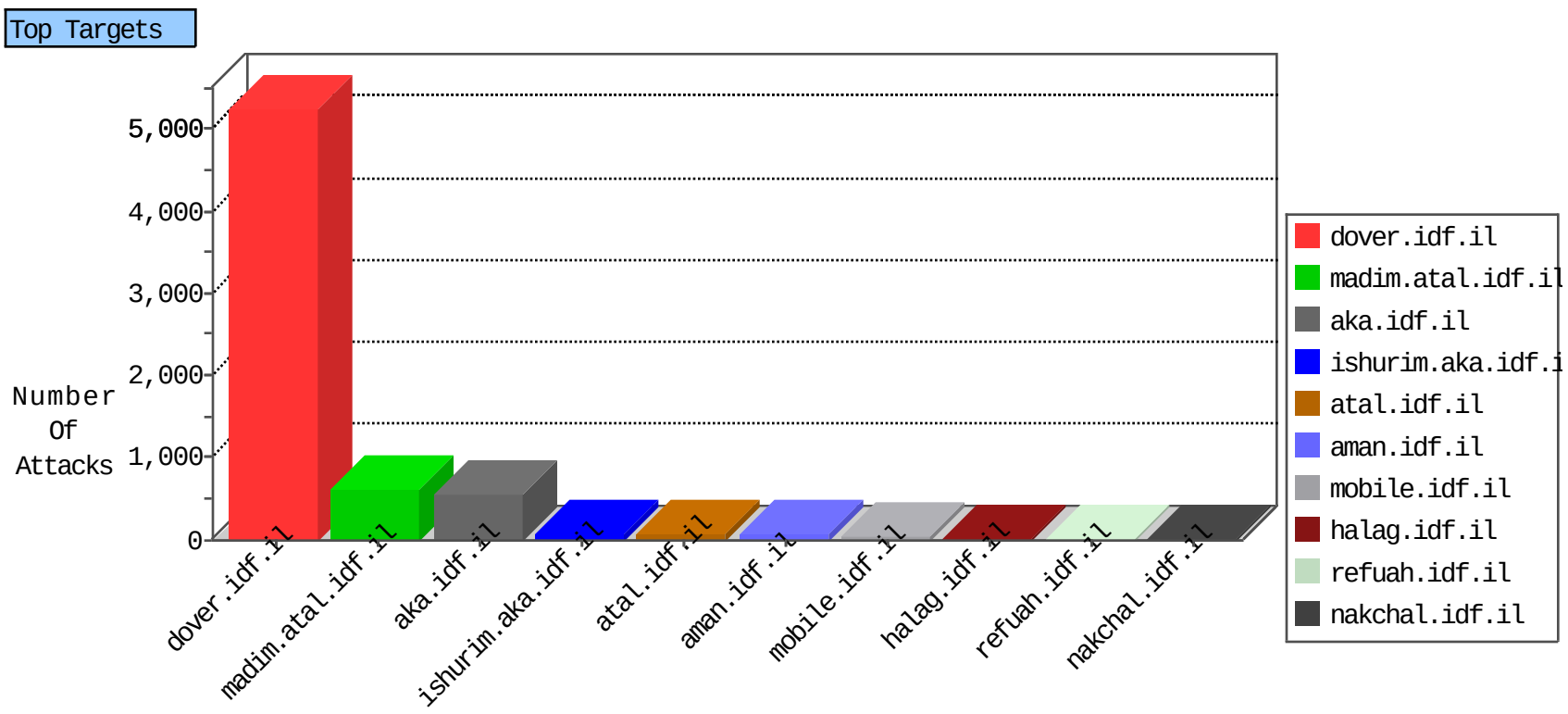
11-25-2015-14:04:04 to 11-25-2015-15:04:04

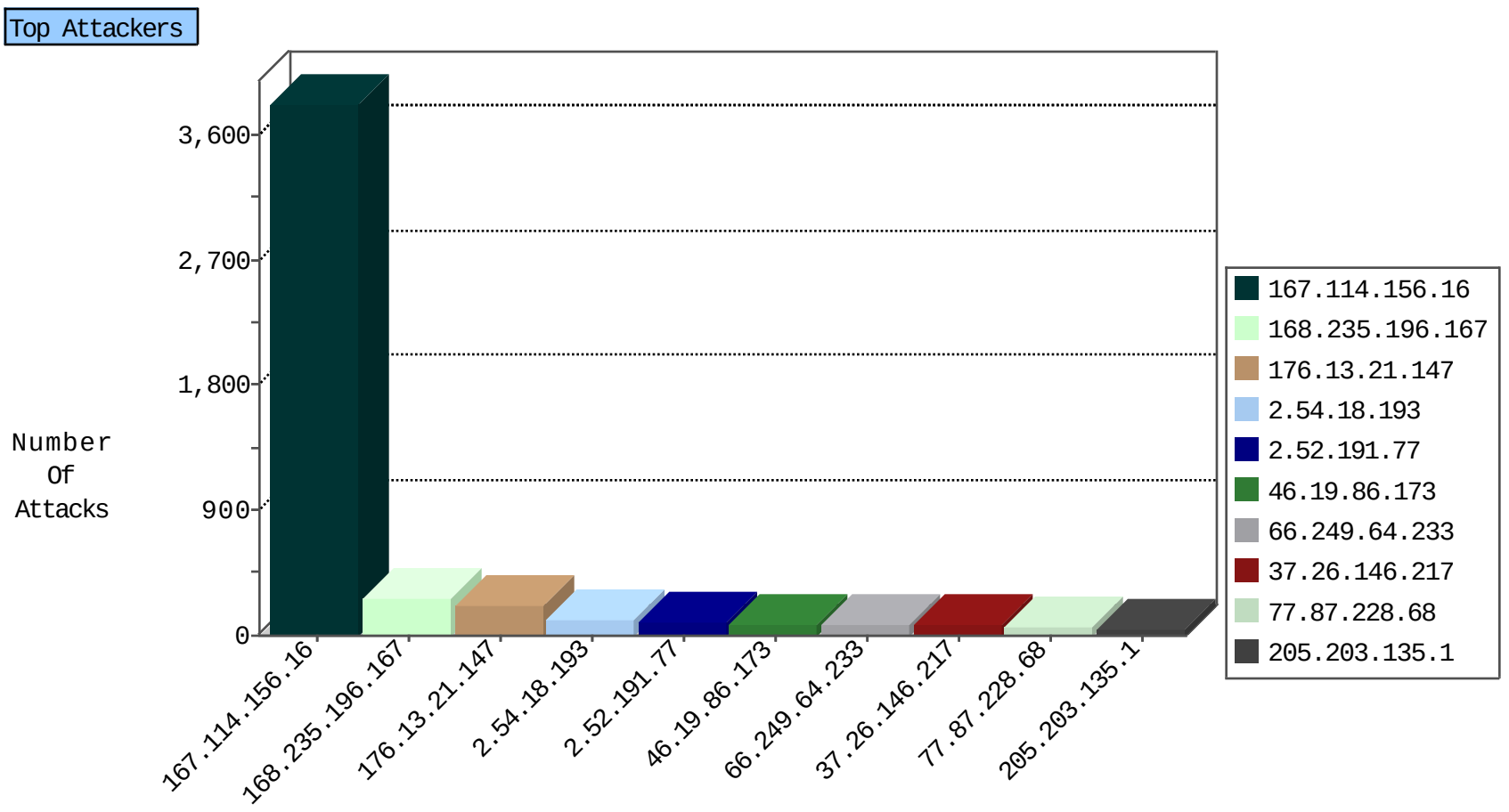
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-25-2015-14:04:04 to 11-25-2015-15:04:04

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	DOS-Tool-SwitchbladG	dest-reset	2573
81.218.37.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
79.178.67.77	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
168.235.196.167	United States	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	3
79.179.155.205	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
84.228.16.196	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
168.235.196.167	United States	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
80.246.130.17	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
61.160.195.6	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
61.182.170.38	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
61.182.170.38	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
104.192.0.226	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
61.182.170.38	China	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

11-25-2015-14:04:04 to 11-25-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.143.54.217	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.116.122.221	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.27	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-25-2015-14:04:04 to 11-25-2015-15:04:04

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
50.204.188.142	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.170.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
91.135.111.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.98.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.38.250.31	147.237.72.156	Greece	aman.idf.il	ET SCAN NMAP -sS window 2048	1
61.244.49.137	147.237.76.34	Hong Kong	yohalan.idf.i	ET SCAN NMAP -sS window 1024	1
31.168.187.140	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
2.52.150.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.74	Sweden	law.idf.il	ET SCAN NMAP -sS window 1024	1
104.243.16.124	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.38.250.31	147.237.72.156	Greece	aman.idf.il	ET SCAN NMAP -sS window 3072	1
62.38.250.31	147.237.72.156	Greece	aman.idf.il	ET SCAN NMAP -f -sS	1

11-25-2015-14:04:04 to 11-25-2015-15:04:04

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	1741
168.235.196.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	268
37.26.146.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
77.87.228.68	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
100.100.101.39		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.14.245		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.82.27		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.109	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	22
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
216.223.27.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
86.145.113.184	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	19
79.179.169.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.64.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
199.30.25.42	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.191	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
216.223.27.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
80.246.130.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
132.76.50.5	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
177.85.47.94	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
216.223.27.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.94.221.138	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
13.17.125.9	United Kingdom	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
216.223.27.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.130.204.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.150.20	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.130.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.175.25	Israel	147.237.77.243	mobile.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
100.100.102.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
185.32.179.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.246.136.218	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.246.130.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
216.223.27.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.203.98.130	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
216.223.27.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
220.255.181.141	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.254.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.22.134.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
149.78.27.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.21.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
176.13.21.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	103
2.54.18.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
2.52.191.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
46.19.86.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
2.52.170.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
2.52.185.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
2.54.18.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
80.246.138.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
37.26.147.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
2.54.4.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.21.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	5
185.32.179.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.175.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	3
176.12.148.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
37.26.147.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.140.204	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.179.155.205	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.12.145.63	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
46.116.122.221	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
5.29.163.189	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/ufi/reaction/	Block	2
212.143.54.217	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
37.142.110.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.254.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.229.72.132	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
176.13.7.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.121.92.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.166.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
221.231.6.246	China	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
46.19.85.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.175.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.217.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-ar/www.idf.il/ar	Block	1
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
87.69.93.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3395.jpg	Block	1
84.110.145.236	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
79.182.11.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.143.54.217	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/1/	Block	1
132.76.61.23	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.125.77.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
197.132.255.147	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1