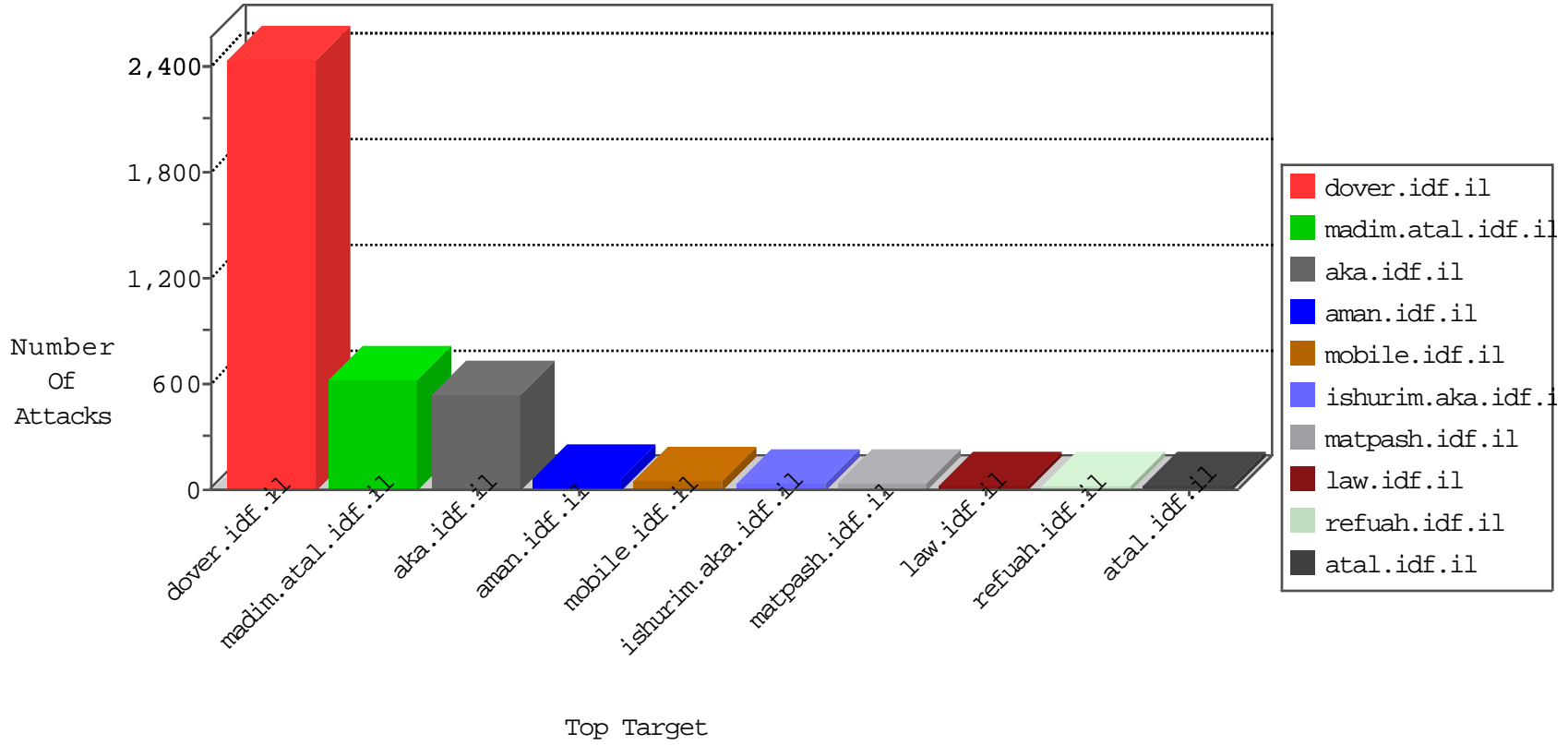


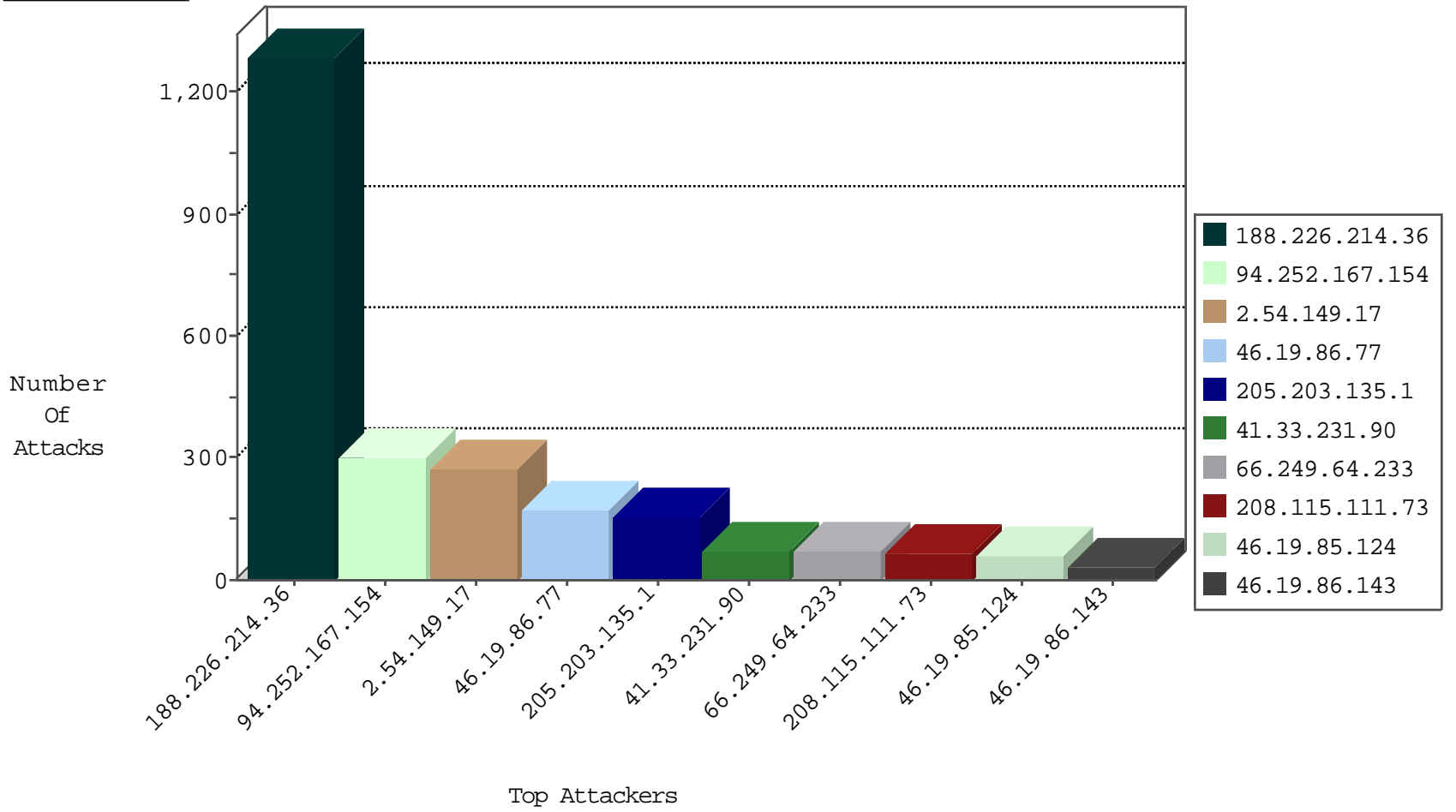
IDF Under Attack Daily Report



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	TCP handshake violation, first packet not syn	drop	172
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
66.249.64.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.8	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	2
80.246.136.163	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
175.10.57.117	China	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
79.176.193.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
46.116.120.179	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.136.163	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
80.74.103.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.199.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.165.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.27.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.30.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.53.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.96.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.1.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.44.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.39.50	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
77.125.150.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
212.150.244.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.72.156	Cote D'Ivoire	aman.idf.il	ET SCAN NMAP -sS window 3072	1
5.29.56.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
144.85.150.128	147.237.77.216	Switzerland	dover.idf.il	ET SCAN NMAP -sS window 4096	1
2.54.39.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.226.214.36	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1288
94.252.167.154	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	291
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
46.19.85.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
213.186.177.29	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
80.246.136.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
107.170.62.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.179.218.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.52.57.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
152.62.109.206	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.168.28.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.199.135.40	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	11
94.252.167.154	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.59.183.105		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
100.100.2.112		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
193.5.216.100	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
155.254.239.157	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
176.12.146.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.66.20.217	Denmark	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
2.52.14.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
81.218.37.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.0	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.49.153.94	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.1.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.66.23.161	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.38	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.11.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.174.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.191	Israel	147.237.77.243	mobile.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
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.77	Block	38
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.149.17	Block	16
2.54.186.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
2.54.129.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
109.105.167.126	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.105.167.126	Block	9
31.186.228.32	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.15.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
31.186.228.58	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
80.246.139.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
31.186.228.31	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.229.55.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.18.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
149.88.233.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.186.228.30	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
31.186.228.94	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.143.3.44	Block	4
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	4
31.186.228.59	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.15.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
192.115.97.253	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
192.115.97.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	3
176.12.145.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.186.228.29	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.186.228.95	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.146.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
31.186.228.60	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.186.228.93	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.186.228.57	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
216.35.195.247	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
109.64.201.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.143.3.44	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
2.54.58.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
1.39.37.148	India	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/gius	Block	2
79.182.189.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
84.109.117.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
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	2
2.54.186.104	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
80.246.136.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.64.201.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1