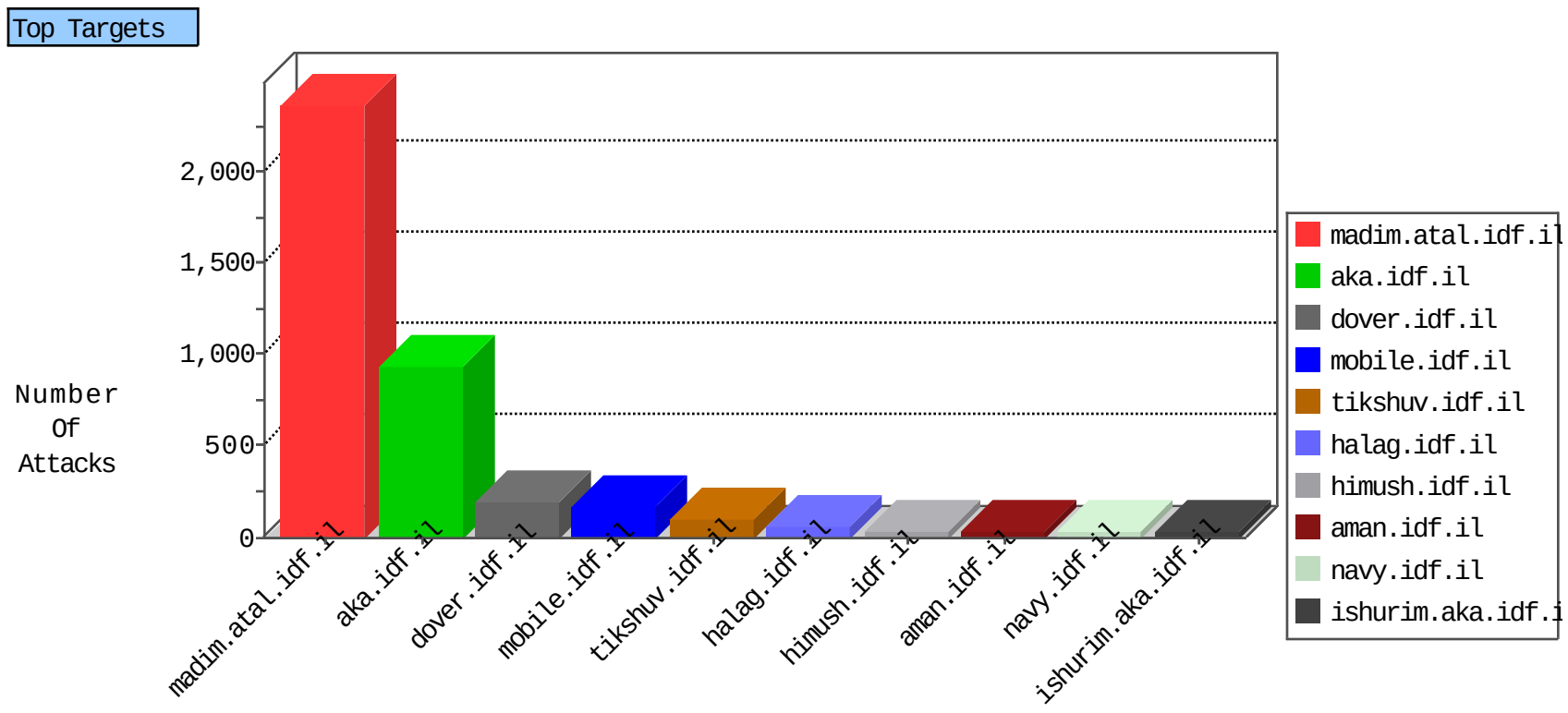
01-31-2016-18:04:09 to 01-31-2016-19:04:09

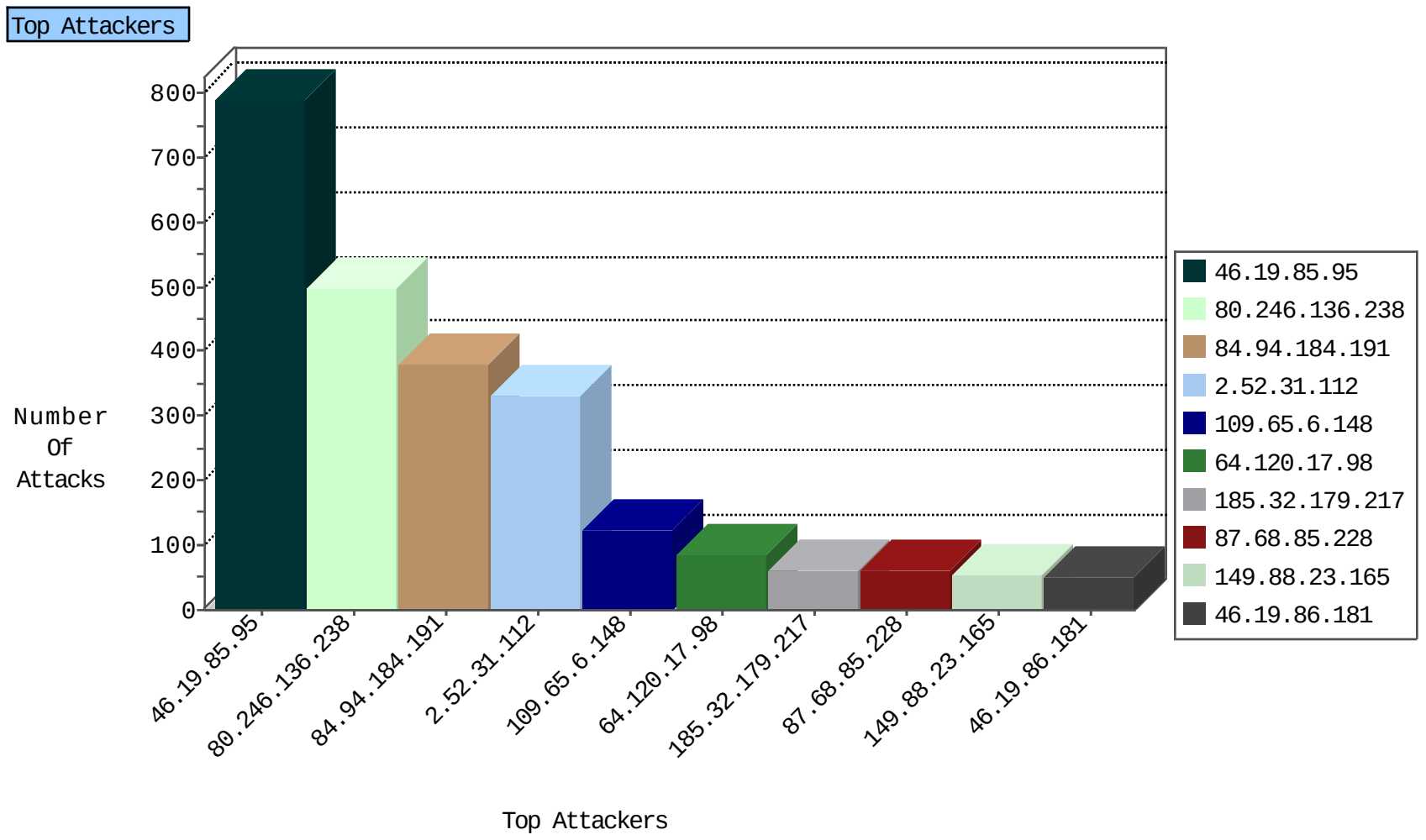
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-31-2016-18:04:09 to 01-31-2016-19:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
66.249.64.50	Israel	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	7
149.78.206.107	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
213.83.135.77	Denmark	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	3
79.182.212.205	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
173.206.138.44	Canada	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
222.173.232.79	China	147.237.72.166	aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
141.212.122.188	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
80.83.237.63	Russian Federation	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	1
37.26.146.229	Israel	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	1
83.101.56.152	Belgium	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	1
45.63.16.166		147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
74.91.28.60	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
105.93.255.70	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

01-31-2016-18:04:09 to 01-31-2016-19:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-31-2016-18:04:09 to 01-31-2016-19:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
80.246.130.143	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
85.64.179.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
210.93.50.130	147.237.0.15	Korea, Republic of	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
31.168.69.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.115.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
64.120.17.98	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
158.130.6.191	147.237.76.202	United States	e.halag.idf.il	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	1
46.121.252.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.216.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.197.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.6.148	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.19.85.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.159.148.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.55.236.147	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.8.28	Morocco	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
80.246.136.238	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
218.246.0.97	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.210.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.219.254.1	147.237.72.156	Mexico	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
27.124.121.194	147.237.0.33	Australia	idf.il	ET SCAN NMAP -sS window 1024	1
77.125.166.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.210.176.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.206.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.218.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.135.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.198.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.153.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.140.253.9	147.237.8.28	Morocco	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
84.108.244.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-31-2016-18:04:09 to 01-31-2016-19:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.6.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	103
64.120.17.98	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
109.253.134.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
185.120.126.39		147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
109.65.109.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
185.32.179.184	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
80.246.130.143	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
80.246.130.143	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.157.127	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
149.88.226.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.155.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
185.32.179.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.121.87	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
64.120.17.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
79.179.58.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.133.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.178.67.141	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.154.94.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.52.173.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
31.154.94.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.57	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.198.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.88.218.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
84.228.180.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.245	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.16.115.22	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.210.186.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.198.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.88.226.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.210.186.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.31.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.17.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.155.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.142.64.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.90.147.211	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	448
80.246.136.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	287
84.94.184.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	244
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	218
80.246.136.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	209
2.52.31.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	174
2.52.31.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	137
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	119
84.94.184.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
87.68.85.228	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
149.88.23.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
185.32.179.217	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.179.217	Block	48
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
176.13.0.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
109.253.216.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
84.94.184.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	29
2.52.31.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	20
79.180.51.53	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
185.32.179.217	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 185.32.179.217	Block	13
85.64.71.167	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.71.167	Block	12
80.246.136.52	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	8
109.67.228.217	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	8
2.54.58.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
109.66.2.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/images/payslips/	Block	7
185.120.126.40		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.223.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.136.52	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	5
176.13.18.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	5
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	4
79.178.226.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	4
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.54.162.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.88.20.168	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	3
46.19.86.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.67.228.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.181.237.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.134.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.217.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.50.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.138.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.157.177	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.57.157.177	Block	3
84.108.50.137	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	3
109.65.6.148	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	2
37.142.228.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.67.160.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.65.6.148	Israel	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	2
109.253.133.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2