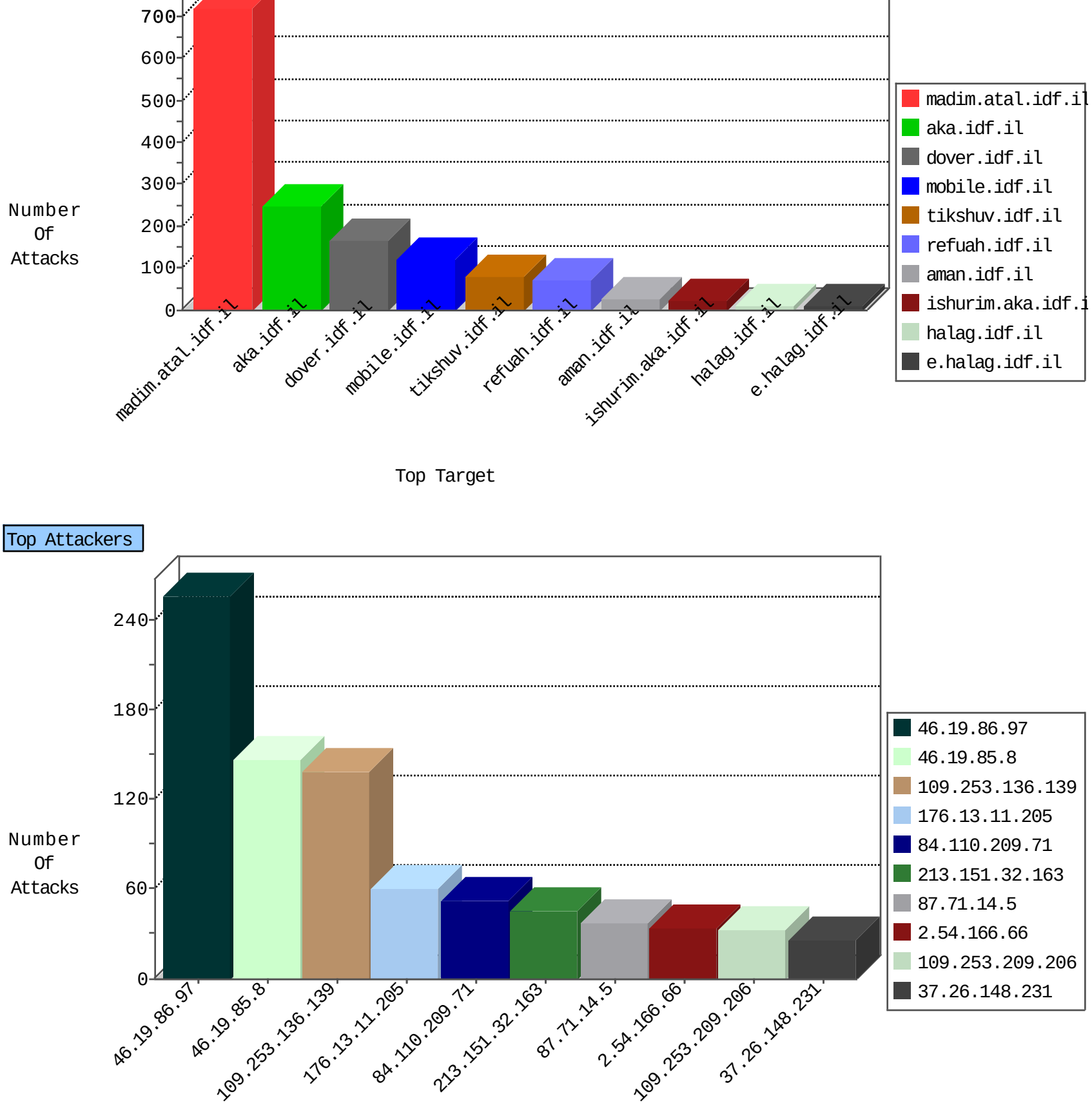
03-03-2016-15:04:06 to 03-03-2016-16:04:06

IDF Under Attack Daily Report



03-03-2016-15:04:06 to 03-03-2016-16:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
84.111.164.68	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
82.145.221.157	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
118.223.194.65	Korea, Republic of	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
67.109.163.18	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
202.58.137.96	Australia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
38.229.1.13	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
164.132.54.194	Italy	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.9	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
52.53.222.9	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
192.171.18.125		147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.57	United States	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
202.58.137.76	Australia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-03-2016-15:04:06 to 03-03-2016-16:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
46.19.86.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.52.39.66	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.52.48.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
91.135.102.188	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.140.152	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.16.163	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.142.210.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.57.75.70	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.210	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
80.246.133.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-03-2016-15:04:06 to 03-03-2016-16:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.114.23.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.35.94.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.111.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.200.142.180	147.237.0.19	Kazakstan	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
79.178.144.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.220.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.74	147.237.76.42	United States	refuah.idf.il	ET DROP Dshield Block Listed Source	1
185.120.125.20	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.244.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.200.142.180	147.237.0.19	Kazakstan	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
79.179.35.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.121	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
218.246.0.97	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.136.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

03-03-2016-15:04:06 to 03-03-2016-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.71.14.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
84.110.209.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
37.26.148.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
85.130.213.204	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
217.132.130.11	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	15
46.19.85.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.110.209.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.54.14.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.173.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
46.120.84.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.105	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.137.80	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.15.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.20.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.119.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
80.246.137.152	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.137.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.110.209.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.110.209.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.250.159.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.166.66	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.168.92.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.86.250	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
68.235.166.183	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.240.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.74.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.244.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.226.28.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.219.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.145.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.228.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.2.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.181.145.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-03-2016-15:04:06 to 03-03-2016-16:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.114.23.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.161.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.84.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	252
46.19.85.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	147
109.253.136.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	138
176.13.11.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
109.253.209.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
2.54.166.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
79.183.151.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
87.70.64.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
37.26.148.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	5
46.19.86.54	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	4
109.253.220.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.71.18.150	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	3
46.210.226.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.186.54.120	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.186.54.120	Block	3
46.19.86.101	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.111.45	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$FAQListViewTemplate1$InternalSearch1$txtFreeTextSearch in www.law.idf.il/327-he/patzar.aspx	Block	3
46.19.86.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.86	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	2
65.55.210.184	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.22.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.95.255.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.186.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.15.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.81.97.48	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/course.aspx	None	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name	Block	1
109.188.125.141	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
37.26.148.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.68.157.105	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.86.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
190.129.96.181	Bolivia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.39.88	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
81.218.50.66	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	NULL Character in Parameter Name	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
37.45.200.41	Belarus	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
91.199.69.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
37.26.146.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
83.130.108.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
40.77.167.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
150.70.188.176	Japan	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.66.136	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/navmenu/	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String	Block	1