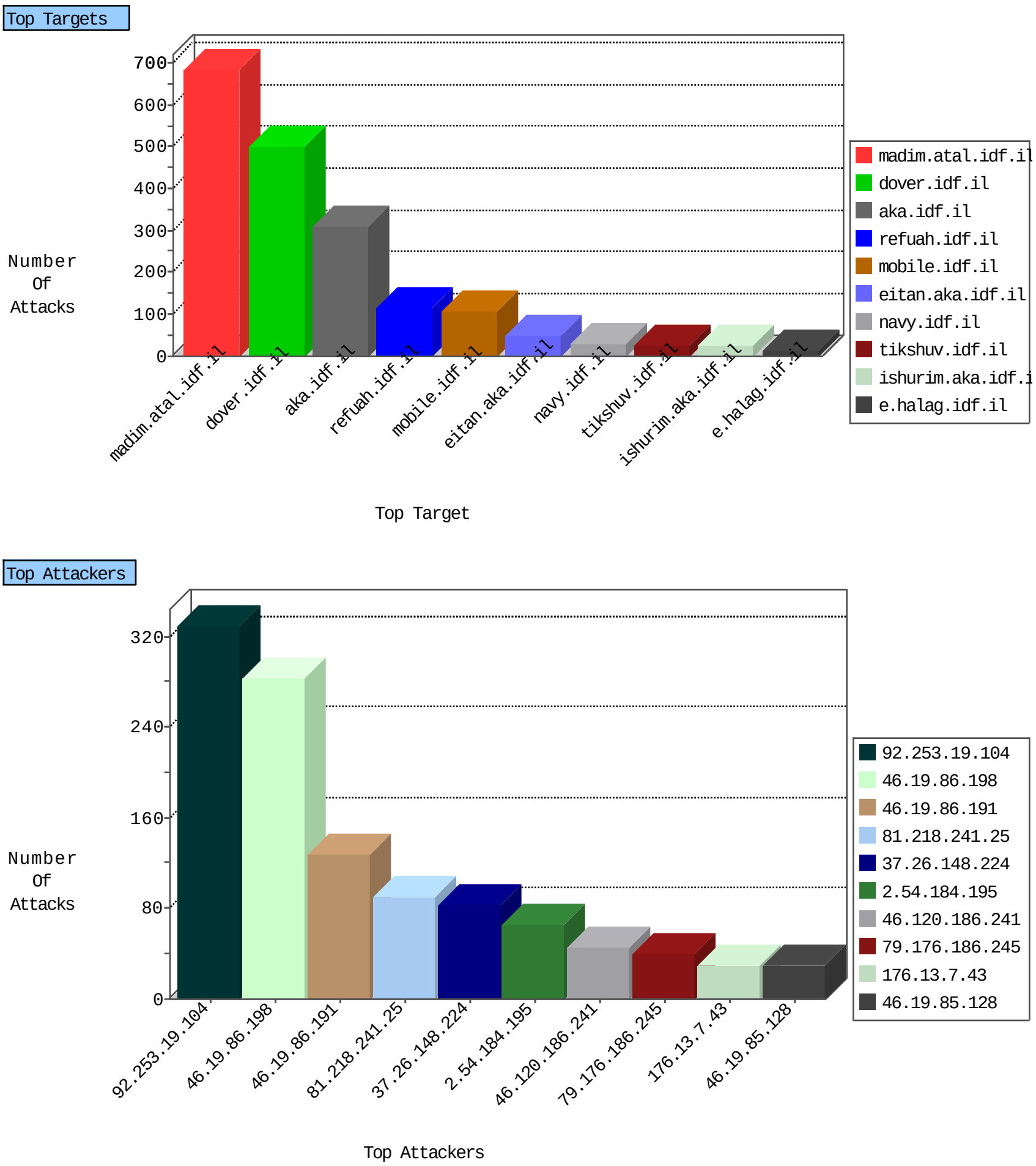
03-07-2016-13:04:01 to 03-07-2016-14:04:01

IDF Under Attack Daily Report



03-07-2016-13:04:01 to 03-07-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	414
92.253.19.104	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	323
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
82.145.218.138	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
80.74.96.29	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
92.253.19.104	Jordan	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
92.253.19.104	Jordan	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
89.248.174.4	Netherlands	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

03-07-2016-13:04:01 to 03-07-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.135.170	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.120.193.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
217.194.207.34	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
151.80.31.151	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	3
5.29.20.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.181.194.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.150	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
2.54.33.202	Israel	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
151.80.31.152	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.153	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-07-2016-13:04:01 to 03-07-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.126.116.147	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
79.176.9.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.252.96.37	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
188.113.209.16	147.237.77.216	Uzbekistan	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.144.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.70.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
17.78.81.100	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.37.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
92.253.19.104	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.105.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.247.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.64.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
62.128.41.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.40.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.115.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
179.32.127.45	147.237.0.17	Colombia	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.149.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.245.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.20.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.103.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.185.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.197.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.36.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-07-2016-13:04:01 to 03-07-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.186.245	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
176.12.135.7	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
176.13.7.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.54.37.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.17.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.12	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
84.229.40.74	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.14.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.153.2	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.57.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
62.0.244.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
194.169.217.122	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.24.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.171.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.171.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.225	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.202.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
78.52.35.108	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.102.9.115	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
79.181.2.62	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
119.139.137.193	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.225	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.166.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.225	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.96	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.211	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
212.179.28.34	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.5	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
82.81.99.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.34.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.152.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.152.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.144.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.2.62	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.67.121.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-07-2016-13:04:01 to 03-07-2016-14:04:01

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.144	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
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	281
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
2.54.184.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
46.120.186.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
109.253.220.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
176.13.7.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
81.1.131.74	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
2.54.139.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
185.32.179.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
81.1.131.74	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.1.131.74	Block	5
80.246.139.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	4
2.54.37.11	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
80.74.103.204	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.74.103.204	Block	4
176.13.12.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.14.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.24.0	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	3
176.13.11.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
40.77.167.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.19.85.37	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
176.13.9.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.111.141.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.143.134.129	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;f in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
132.71.160.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
216.218.206.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
94.230.93.33	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
199.30.25.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.251.251	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
79.181.209.129	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
51.254.44.137	United Kingdom	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
2.54.171.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.65.188.226	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
212.143.134.129	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;rnd in www.eitan.aka.idf.il/shared/ajax/createcaptchaimage.aspx	None	1
41.47.105.54	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
185.82.200.91		147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
80.246.139.198	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1