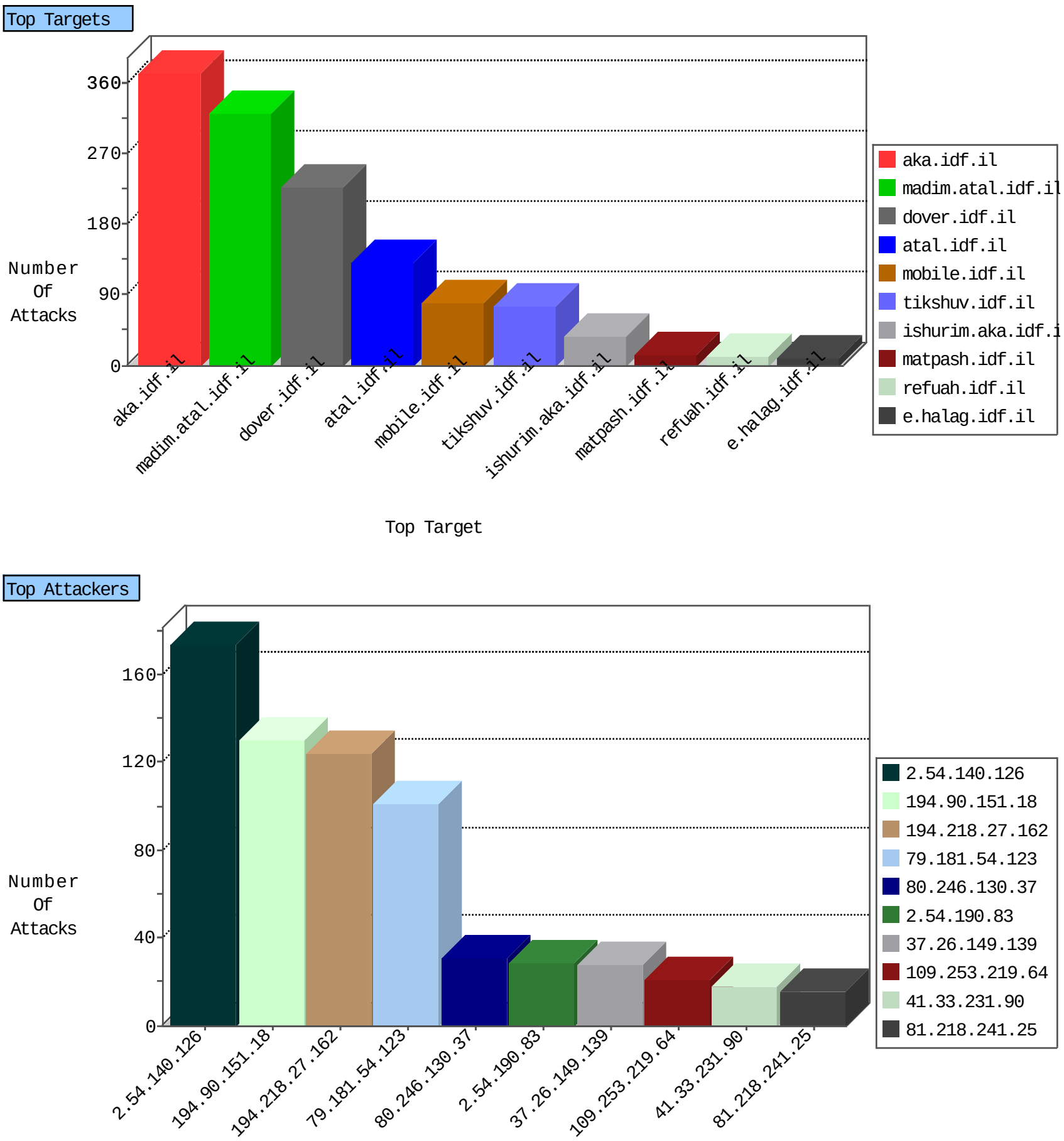
03-02-2016-14:04:01 to 03-02-2016-15:04:01

IDF Under Attack
Daily Report



03-02-2016-14:04:01 to 03-02-2016-15:04:01

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	93
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
192.99.63.194	Canada	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
192.99.63.194	Canada	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
212.118.253.117	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
192.99.63.194	Canada	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
61.85.222.199	Korea, Republic of	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
164.132.54.194	Italy	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
192.99.63.194	Canada	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.9	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
164.132.54.194	Italy	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1

03-02-2016-14:04:01 to 03-02-2016-15:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.50.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
176.228.30.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.250.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
195.154.187.115	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
212.143.57.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
195.154.187.115	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.4.148	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
195.154.187.115	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
157.55.39.210	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
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	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-02-2016-14:04:01 to 03-02-2016-15:04:01

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	2
2.54.148.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.143.232.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.17.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.199.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.134.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.212	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.1.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.250.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.226.22.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.137.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.254.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.94.40.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.95.48.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.104.109	147.237.77.176	Israel	matpash.idf.il	ET SCAN NMAP -sA (2)	1
79.181.231.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.76.111.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.194.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.162.26.4	147.237.72.166	Spain	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.209	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
113.76.90.49	147.237.77.61	China	e.cogat.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
37.26.149.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.222.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.72.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.156.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-02-2016-14:04:01 to 03-02-2016-15:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.90.151.18	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	93
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	84
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	40
194.90.151.18	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	31
80.246.130.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
2.54.190.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.219.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
84.110.36.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.38.222	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.102.9.115	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
62.0.218.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.55.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.214.193	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.23.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.205.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.241.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.99.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.140.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.151.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.136.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.130.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.100	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.151.47.159	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.131.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.149.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.39.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.1.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.164.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.205.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.130.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.3.233	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.183.103.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.25.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.26.149.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.97.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.179	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-02-2016-14:04:01 to 03-02-2016-15:04:01

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
167.220.196.178	United Kingdom	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
2.54.140.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	174
79.181.54.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	15
109.253.200.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
2.54.3.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.54.190.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
147.236.238.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
85.130.131.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	4
2.54.12.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.83.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.139.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.219.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	3
84.228.242.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
5.29.205.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.52.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.13.100.112	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.11.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.78.153	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainpniot/	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request method	Block	1
107.150.42.37	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
46.19.86.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.52.0.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Malformed URL ¯-p' ¦f¯pÐ~z¡c[[#5]]ev˙.[[#6]]א´ס^Š	Block	1
31.168.138.81	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.159.159.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
2.54.50.147	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
109.66.114.101	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
85.64.68.134	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.52.164.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/6_s3_	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Unknown HTTP Request Method ²[[#8]]ÊæM÷5[[#25]][[#17]]″Íe€È™ in URL ¯-p' ¦f¯pÐ~z¡c[[#5]]ev˙.[[#6]]א´ס^Š	Block	1
66.249.83.161	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
147.236.238.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	1
213.151.47.159	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/1100-8214-he/eitan.aspx	None	1