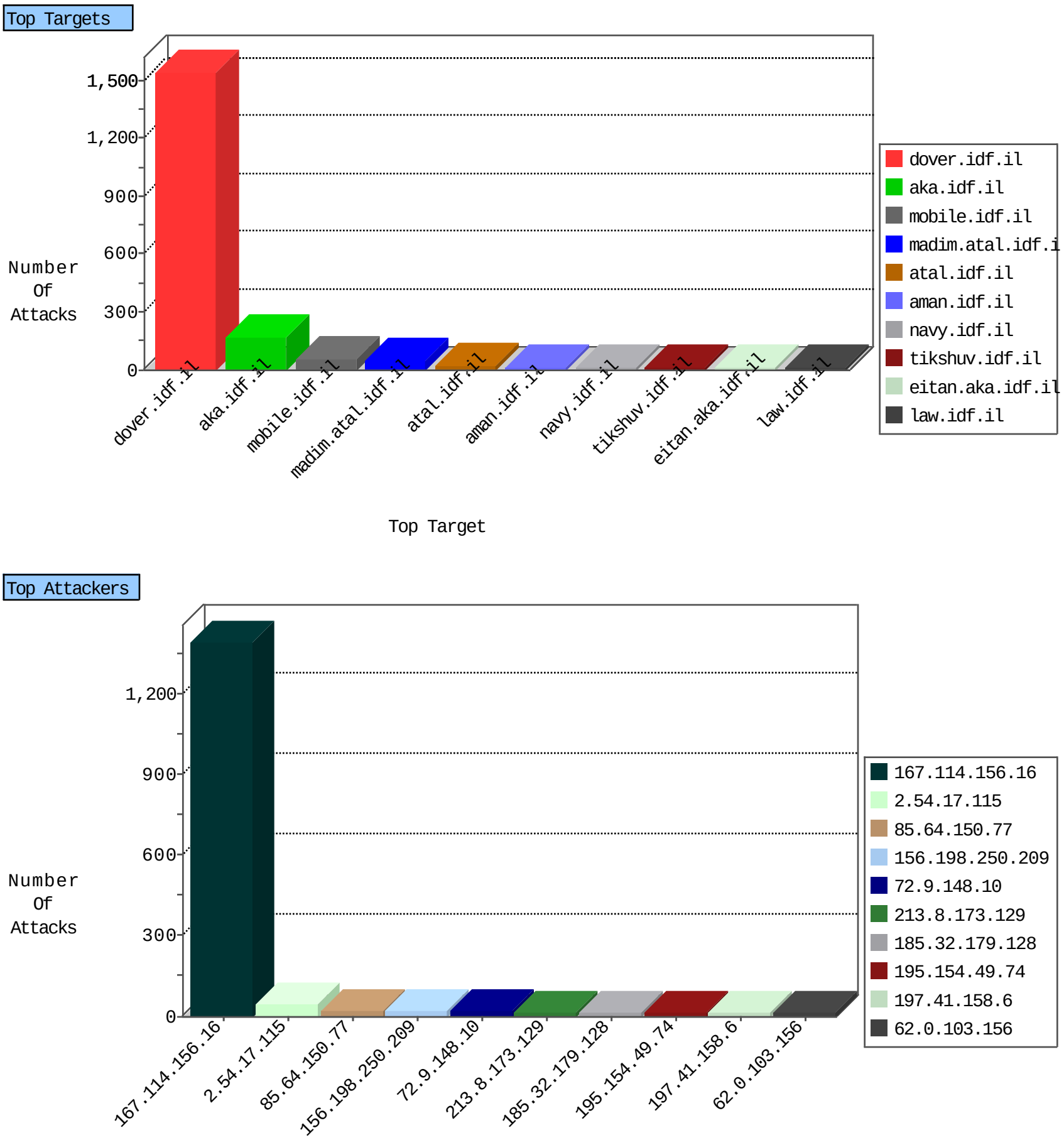
03-12-2016-22:04:09 to 03-12-2016-23:04:09

IDF Under Attack Daily Report



03-12-2016-22:04:09 to 03-12-2016-23:04:09

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	DOS-Tool-SwitchbladG	dest-reset	3972
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
200.160.6.137	Brazil	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.248.162.146	Netherlands	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
89.248.162.146	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
89.248.162.146	Netherlands	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1

03-12-2016-22:04:09 to 03-12-2016-23:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.79.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
107.150.56.254	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
109.64.188.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-12-2016-22:04:09 to 03-12-2016-23:04:09

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	4
66.249.93.95	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.91	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.194	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.76.201	France	e.atal.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.77.74	Austria	law.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.76.199	France	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
195.154.49.74	147.237.76.38	France	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
52.33.232.198	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
195.154.49.74	147.237.8.28	France	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
40.117.103.99	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.0.16	France	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.139.27.231	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
192.3.9.122	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1
195.154.49.74	147.237.77.205	France	prisha.idf.il	ET SCAN Potential SSH Scan	1
192.3.9.122	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
195.154.49.74	147.237.77.178	France	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
137.226.113.7	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
195.154.49.74	147.237.77.74	France	law.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.77.216	Austria	dover.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.76.200	France	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.77.61	Austria	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.76.177	France	ncore.idf.il	ET SCAN Potential SSH Scan	1
195.154.49.74	147.237.8.45	France	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
52.33.232.198	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
37.139.27.231	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
192.3.9.122	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
195.154.49.74	147.237.77.179	France	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
173.193.139.2	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.77.170	France	maarachot.idf.il	ET SCAN Potential SSH Scan	1

03-12-2016-22:04:09 to 03-12-2016-23:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.64.150.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
213.8.173.129	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
185.32.179.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.110.211.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.130.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.17.115	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
186.27.142.2	Colombia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
87.71.68.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
156.198.250.209		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.198	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
197.41.158.6	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.219.155.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.60.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.116.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.179.160.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
156.198.250.209		147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
79.179.121.162	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
62.0.103.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
197.41.158.6	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
91.200.12.106	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
5.102.254.3	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
79.182.13.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.209.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.183	United States	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.206.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.167.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.229.34.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.60.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.164.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.173.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
156.198.250.209		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.60.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.207.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.86.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.162.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.194.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.29.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
156.198.250.209		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.210.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-12-2016-22:04:09 to 03-12-2016-23:04:09

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.26.148.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.0.103.156	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
84.108.18.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.169.159	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
2.54.17.115	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	26
85.64.150.77	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
2.54.17.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.51.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
65.55.210.157	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
62.0.103.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.65.247.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.128	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
5.22.135.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/giys	Block	2
79.181.1.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.120.148.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catID in www.aka.idf.il/giyus/forms/downloadform.asp	None	1
213.8.173.129	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.60.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.32.179.128	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 185.32.179.128	Block	1
94.230.93.55	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
71.185.67.214	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.117.253.205	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
85.250.110.106	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
213.8.173.129	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
94.230.93.61	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.225.131.141	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
137.226.113.7	Germany	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
94.52.190.196	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.83.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.120.125.27		147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
23.96.208.27	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	1
95.86.83.155	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/https:/madim.atal.idf.il/	Block	1
79.183.177.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.253.181.41	Turkey	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.66.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	1
185.6.59.134	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.52.190.196	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.83.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
186.27.142.2	Colombia	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.15.10.37	Czech Republic	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
95.86.83.155	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.83.155	Block	1
84.111.188.182	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/69423.pdf	Block	1
212.253.181.41	Turkey	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
185.32.179.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
94.230.93.48	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.93.94	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1