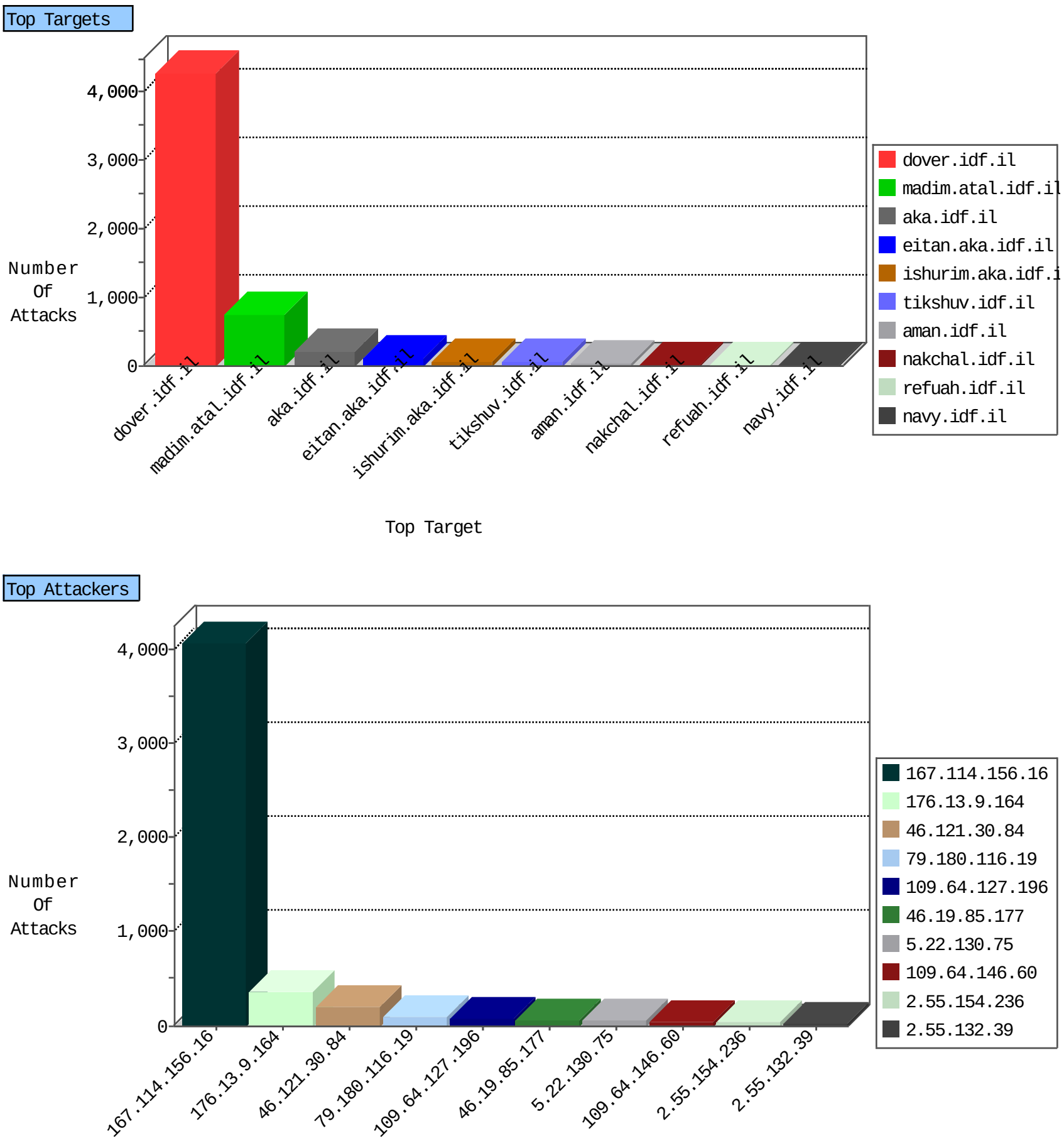
04-18-2016-18:04:05 to 04-18-2016-19:04:05

IDF Under Attack Daily Report



04-18-2016-18:04:05 to 04-18-2016-19:04:05

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	Block_Ip_Web_In	drop	4063
41.239.7.110	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
109.64.12.74	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.177.128.141	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
31.168.14.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
107.150.32.62	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
74.91.23.106	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
69.30.226.98	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2
69.30.198.147	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
74.91.20.194	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	2
69.30.202.226	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
107.150.32.59	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
74.91.20.197	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
69.30.202.228	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
159.122.220.135	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
52.28.32.164	Germany	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Https	drop	1
159.104.163.19	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.122.220.135	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
159.104.163.20	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.122.220.135	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
159.104.163.17	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
52.28.32.164	Germany	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Https	drop	1
159.122.220.135	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
159.104.163.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

04-18-2016-18:04:05 to 04-18-2016-19:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-18-2016-18:04:05 to 04-18-2016-19:04:05

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	1

04-18-2016-18:04:05 to 04-18-2016-19:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.9.164	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	162
109.64.127.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
176.13.9.164	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	80
5.22.130.75	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
109.64.146.60	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
82.73.45.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
93.173.189.129	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
2.55.132.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
2.55.154.236	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
212.179.40.171	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
24.114.223.254	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
94.234.170.42	Sweden	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.168.89.228	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.137	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.137	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.70.45.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.66.23.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.13.176	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
46.19.85.191	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.68.30.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.154.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.200.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.154.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.8.80.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.105.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.136.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.154.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.179.209.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.7.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.55.154.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.55.132.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.26.180.142	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.195.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.182.188.22	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
5.102.254.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.242.38	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.84.208	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.53.24.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.176.84.208	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.176.84.208	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.236.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.13.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

04-18-2016-18:04:05 to 04-18-2016-19:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
149.78.25.226	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.61.104	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
46.121.30.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	207
176.13.9.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
79.180.116.19	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	54
79.180.116.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
192.116.1.73	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	7
204.154.185.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
109.253.224.227	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.224.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.113.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.121.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
80.82.78.38	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
74.91.23.106	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
217.132.84.43	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
2.53.154.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
69.30.226.99	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3156.jpg	Block	1
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
84.111.85.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.209.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.179.209.37	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
132.66.23.64	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
79.181.12.236	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.28.166.82	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
74.91.20.194	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/menu-ending.gif	Block	1
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_ses.20.8afc=*	Block	1
105.225.231.141	South Africa	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
79.179.209.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/giyus	Block	1
69.30.198.147	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.app-softwares.com/	Block	1
132.66.96.43	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/580-he/patzar.aspx	Block	1
46.121.30.84	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.182.188.22	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
5.28.166.82	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
74.91.20.197	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method k_id.20.8afc=443afcd340d0c33b.1460994657.1.1460994657.1460994657.; in URL _pk_ses.20.8afc=*	Block	1
107.150.32.62	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
69.30.202.228	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
149.88.114.202	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal/site/templates/controller.asp	Block	1
66.220.145.246	United States	147.237.72.166	aka.idf.il	Post Request - Missing Content Type	Block	1
80.82.78.38	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
74.91.20.198	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19666-he/idfgdover.aspx	Block	1
204.154.186.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.129	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
69.30.226.98	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.369bs.com/	Block	1
157.55.39.90	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1