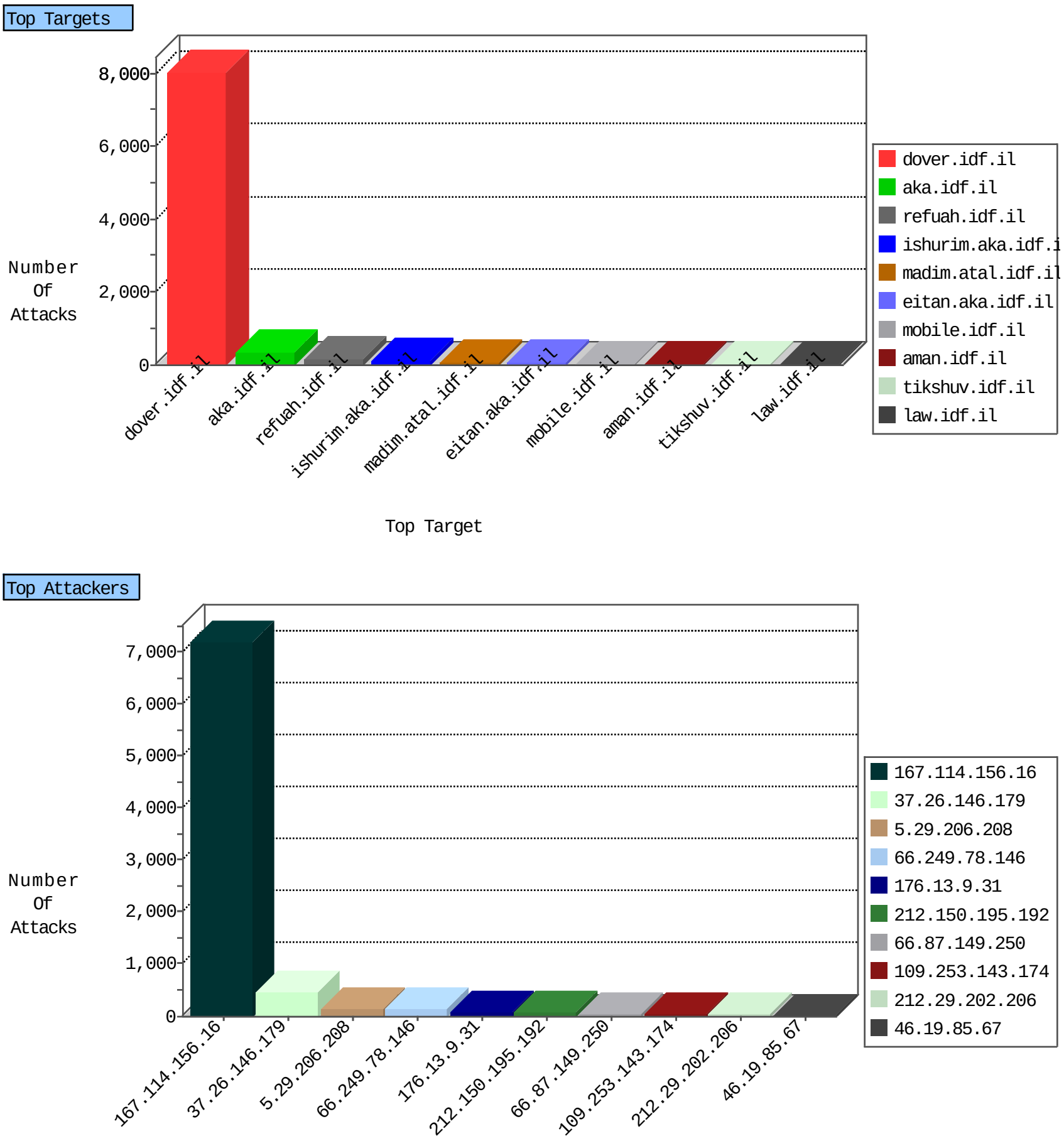
04-24-2016-15:04:03 to 04-24-2016-16:04:03

IDF Under Attack Daily Report



04-24-2016-15:04:03 to 04-24-2016-16:04:03

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	HTTP-POST-Segmented-DoS	dest-reset	12502
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6708
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	544
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	38
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
118.114.23.180	China	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
175.11.237.220	China	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
121.8.125.59	China	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
180.114.97.83	China	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
5.196.199.231	France	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
180.115.35.91	China	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
153.227.196.172	Japan	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
58.34.90.139	China	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
169.54.244.75	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
182.100.12.187	China	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
60.179.13.69	China	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1

04-24-2016-15:04:03 to 04-24-2016-16:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.186.243.91	Jordan	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	2
91.186.243.91	Jordan	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
177.185.194.45	Brazil	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

04-24-2016-15:04:03 to 04-24-2016-16:04:03

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

04-24-2016-15:04:03 to 04-24-2016-16:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6866
37.26.146.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	469
5.29.206.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	130
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	129
212.150.195.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
176.13.9.31	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
66.87.149.250	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
212.29.202.206	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
117.246.184.118	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
85.130.251.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.165.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.20.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.9.31	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
82.145.210.167	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.72	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.185.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
141.0.15.21	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.53.20.37	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.53.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.171.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.22.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.71.112.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.12	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.85.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.186.243.91	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.154.251.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.145.220.192	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.188.139.81	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.9.31	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
91.186.243.91	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
207.232.21.105	Israel	147.237.0.33	idf.il	drop		drop	5
82.213.32.185	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
89.138.103.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.182.33.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.14.50.146	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.174	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		alert	4
79.176.65.53	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.148.174	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.143.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
91.186.243.91	Jordan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.186.243.91	Block	5
109.253.147.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.204.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.160.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.234.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/9/	Block	3
85.4.138.98	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage.asp	Block	2
80.246.139.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.66.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
46.116.14.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/mobile	Block	1
141.212.122.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /x	Block	1
198.20.87.98	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.167/	Block	1
66.249.66.44	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/yoman.asp	Block	1
5.29.206.208	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
91.186.243.91	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/abc123/	Block	1
176.13.20.175	Israel	147.237.72.166	aka.idf.il	Extremely Long Parameter in www.aka.idf.il ðŸŒ¸×¤×¡×– ×©×ž×—ðŸŒ¸ ðŸŒ¸×¤×¡×– ×©×ž×—ðŸŒ¸ ðŸŒ¸×¤×¡×– ×©×ž×—ðŸŒ¸ ðŸŒ¸×¤×¡×– ×©×ž×—ðŸŒ¸ ðŸ	Block	1
87.70.53.246	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.103	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
66.249.66.47	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
93.173.229.233	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
82.81.18.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
176.13.21.84	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/m/templates/getfile/getfile.aspx	Block	1
87.71.112.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.aspx)	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
141.212.122.129	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /x	Block	1
93.173.235.50	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.234.19	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	1
178.141.135.228	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
120.132.50.135	China	147.237.77.19	law-forum.idf.il	Suspicious Response Code	Block	1
89.139.156.112	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_FINISH)	None	1
77.125.111.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catld in www.aka.idf.il/main/giyus/general.aspx	None	1
216.189.160.215	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.201	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
141.212.122.129	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	1
104.251.90.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
184.105.247.195	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
2.53.164.202	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
120.147.144.74	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
79.180.232.27	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1

04-24-2016-15:04:03 to 04-24-2016-16:04:03