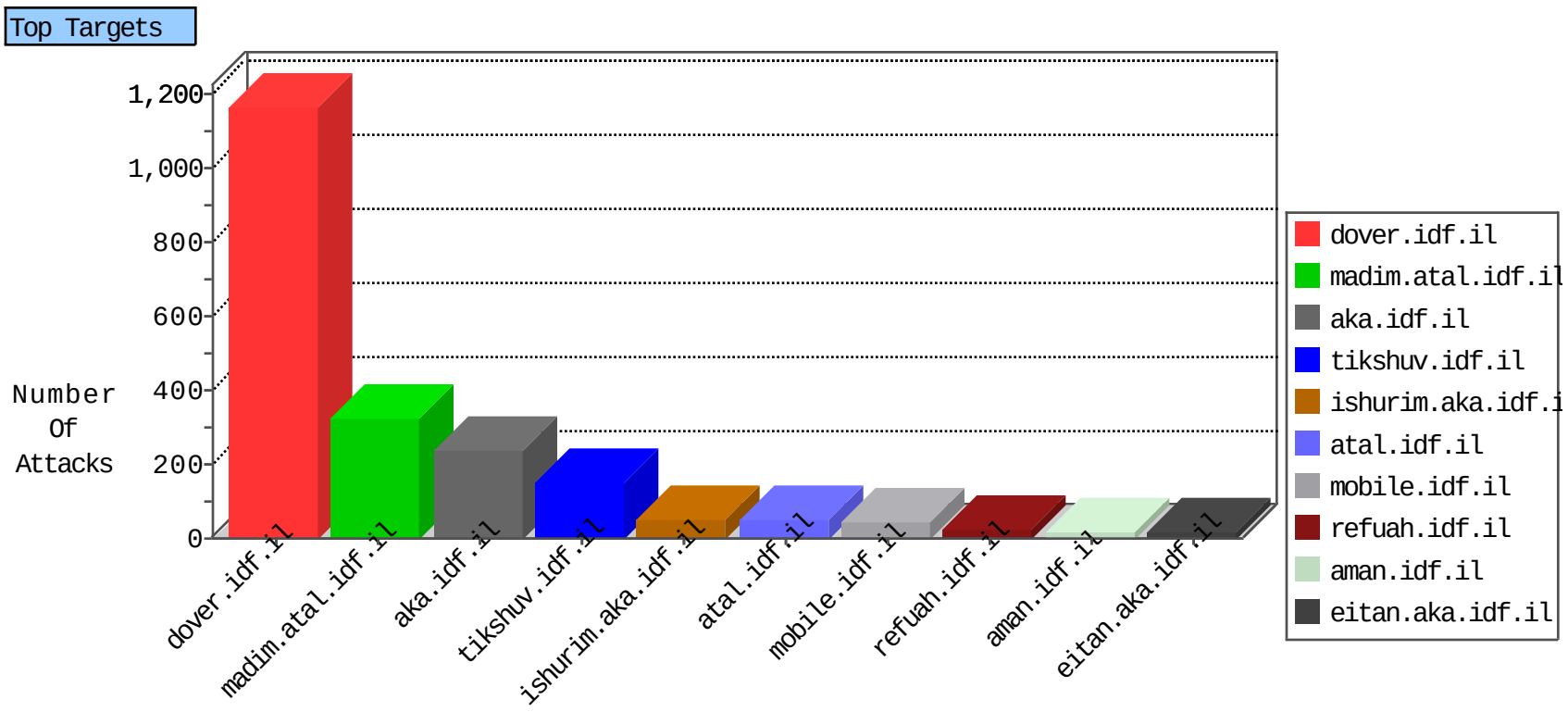
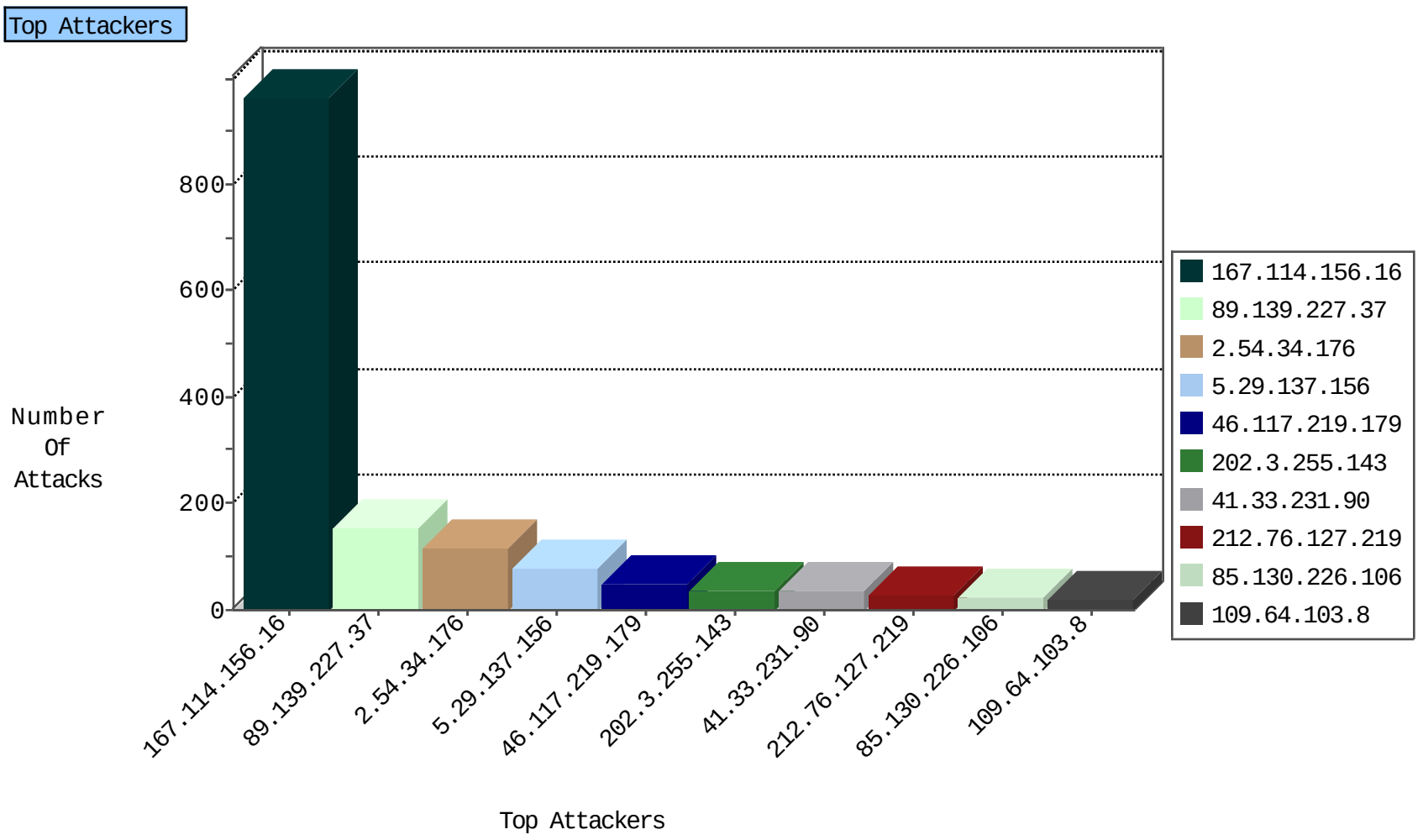
01-16-2016-19:04:08 to 01-16-2016-20:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-16-2016-19:04:08 to 01-16-2016-20:04:08

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	3000
23.16.77.102	Canada	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	2
5.189.169.162	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
142.54.169.164	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
45.32.183.57		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
5.189.169.162	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
112.222.159.198	Korea, Republic of	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
5.189.169.162	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
5.189.169.162	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
151.80.109.172	Italy	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
45.32.183.57		147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
5.189.169.162	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
5.189.169.162	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
5.189.169.162	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
69.9.146.192	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
5.189.169.162	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
142.54.169.164	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
5.189.169.162	Germany	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
74.91.28.60	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
5.189.169.162	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

01-16-2016-19:04:08 to 01-16-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.79.86.129	Netherlands	147.237.77.216	dover.idf.i	3886: HTTP: Cross Site Scripting in POST Request	Block	1
197.0.148.107	Tunisia	147.237.77.216	dover.idf.i	C1000205: HTTP: Opisrael 2015 - key words and groups	Block	1
149.202.47.161	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
197.0.40.226	Tunisia	147.237.77.216	dover.idf.i	3886: HTTP: Cross Site Scripting in POST Request	Block	1
197.0.148.107	Tunisia	147.237.77.216	dover.idf.i	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
197.0.148.107	Tunisia	147.237.77.216	dover.idf.i	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	1

01-16-2016-19:04:08 to 01-16-2016-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

01-16-2016-19:04:08 to 01-16-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
85.130.226.106	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.64.103.8	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
5.22.130.252	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.196	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
79.181.142.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.164.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.9	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.117.9.118	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
2.54.85.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.47.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.46.39.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.138.59	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.29.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.138.59	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.210.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.21.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.131.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.156.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
132.64.210.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.17.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.45	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
85.64.148.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.177.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.181.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.28.153.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
130.203.136.75	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
84.228.215.105	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.135.118	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.46.39.104	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.101.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.198.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.109.50.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.166.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.147.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.187.210	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.20.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.10.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.98.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.99.204	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.171.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.14.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-16-2016-19:04:08 to 01-16-2016-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.34.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
89.139.227.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
5.29.137.156	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	79
89.139.227.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	57
46.117.219.179	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.219.179	Block	48
2.54.34.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
80.246.137.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
109.253.209.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
85.64.151.138	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
46.19.85.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
79.182.197.84	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/sip_storage/files/0/2940.pdf-	Block	5
197.0.40.226	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.0.40.226	Block	4
149.88.58.65	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	4
197.0.24.189	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.0.24.189	Block	4
5.79.86.129	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.79.86.129	Block	4
5.102.253.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
197.0.148.107	Tunisia	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
84.108.166.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.125.112.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.29	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	2
197.0.148.107	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.0.148.107	Block	2
85.65.113.10	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
84.108.146.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.197.84	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.182.197.84	Block	2
109.253.223.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.102.253.90	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
46.19.86.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.149.147	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
197.0.24.189	Tunisia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
5.254.97.103	Romania	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
80.246.138.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.22.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.213.175	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.182.213.175	Block	2
5.254.97.103	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/	Block	2
79.182.171.112	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.142.64.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.0.24.189	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/wp-admin	Block	1
5.79.86.129	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/	Block	1
87.69.180.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
85.64.119.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.17.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.76.15.13	China	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
149.88.58.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.216.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
31.154.153.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.178.102.111	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.243	Block	1

01-16-2016-19:04:08 to 01-16-2016-20:04:08