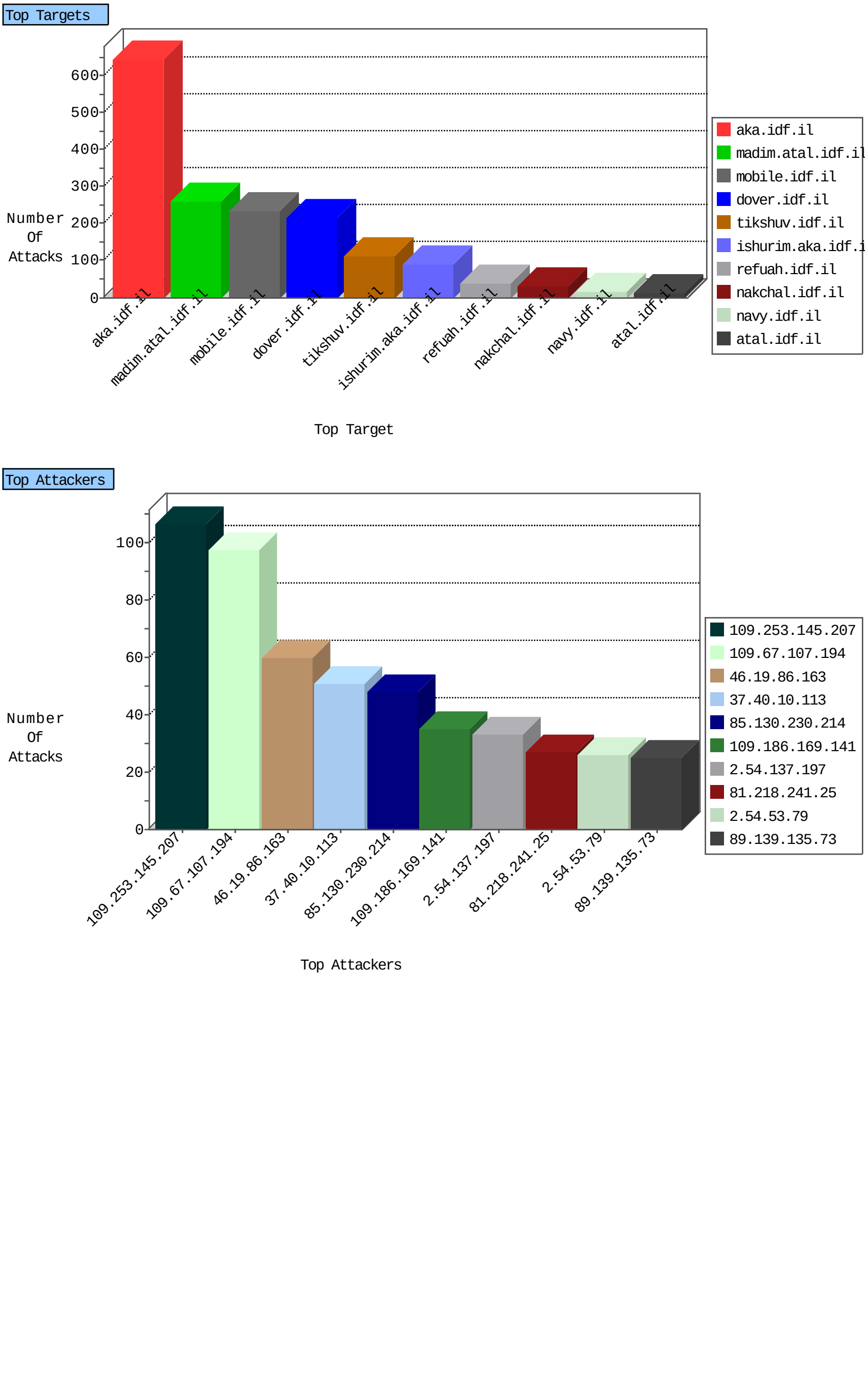
02-03-2016-13:04:05 to 02-03-2016-14:04:05

IDF Under Attack Daily Report



02-03-2016-13:04:05 to 02-03-2016-14:04:05

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	108
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
58.97.111.10	Thailand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
153.232.222.163	Japan	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
58.97.111.9	Thailand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

02-03-2016-13:04:05 to 02-03-2016-14:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.203.196.253	Israel	147.237.72.166	aka.idf.il	14062: HTTP: SpamBlockerUtility Fake Anti-Spyware User-Agent (SpamBlockerUtility x.x.x)	Block	2
88.150.221.26	United Kingdom	147.237.77.216	dover.idf.i	C008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-03-2016-13:04:05 to 02-03-2016-14:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
147.236.232.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
91.142.174.82	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
89.139.22.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.157.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.57.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.37	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
217.194.197.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.148.22.26	147.237.77.178	Lithuania	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.52.63.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.142.174.82	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN Potential SSH Scan	1
91.142.174.82	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
85.250.190.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.0.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.218.11.69	147.237.77.216	Switzerland	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
71.94.154.94	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.165.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.144.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.238.230.133	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

02-03-2016-13:04:05 to 02-03-2016-14:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.230.214	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.86.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	47
37.40.10.113	Oman	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
109.186.169.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
109.253.209.218	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.53.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
31.168.173.2	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
46.120.50.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.54.10.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.40.10.113	Oman	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
109.253.136.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
176.13.15.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
89.139.135.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.103	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
194.90.153.50	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.155.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.136.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.40.10.113	Oman	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7
46.19.85.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.63.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.156.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.213.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.193	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.59.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.39.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.50.90	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
81.4.163.106	Cyprus	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.238.55	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
176.13.1.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.96.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.170	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.238.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.108.34.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.197.203	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.210	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
93.184.15.192	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
109.253.197.203	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

02-03-2016-13:04:05 to 02-03-2016-14:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.137.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.54.131.192	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

02-03-2016-13:04:05 to 02-03-2016-14:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.107.194	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
109.253.145.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
2.54.137.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
80.246.137.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
2.54.13.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
109.253.145.207	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.145.207	Block	17
80.246.136.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
46.19.86.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
109.253.158.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
89.139.135.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
37.142.222.233	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.142.222.233	Block	11
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
149.88.120.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/registrationwizard/undefined	Block	10
109.186.169.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
109.253.159.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
87.69.67.209	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/questionnaire.aspx	Block	5
2.54.53.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
80.246.136.32	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.246.136.32	Block	5
176.13.15.68	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
87.69.67.209	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.67.209	Block	4
2.54.41.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.136.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.179.207.138	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	3
213.8.204.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim	Block	3
2.54.10.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.169.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$116 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.140.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$87 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
80.246.136.32	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1540	Block	2
79.180.63.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$78 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.253.136.53	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.65.223.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
149.50.82.180	United States	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$81 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
176.13.16.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.52.61.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
77.126.117.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.65.34.141	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
95.86.68.120	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$112 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.11.69	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.179.59.204	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.253.216.17	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$116 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
85.65.223.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$76 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
84.108.65.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
217.132.158.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$120 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.85.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$81 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.180.15.238	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in aka.idf.il/main/giyus/questionnaire.aspx	None	1

02-03-2016-13:04:05 to 02-03-2016-14:04:05

02-03-2016-13:04:05 to 02-03-2016-14:04:05