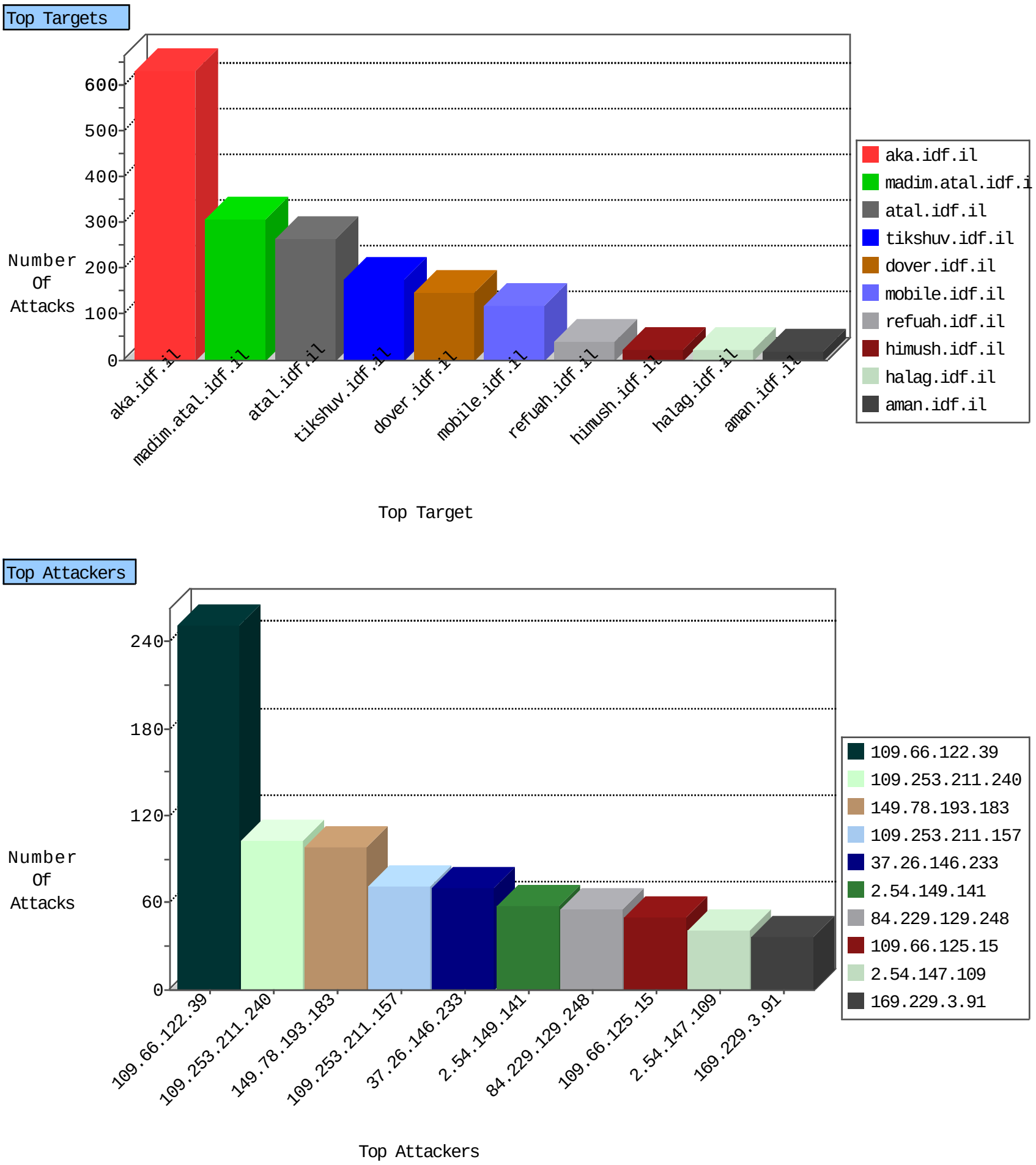
02-03-2016-15:04:00 to 02-03-2016-16:04:00

IDF Under Attack Daily Report



02-03-2016-15:04:00 to 02-03-2016-16:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
79.178.136.75	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
113.128.102.15	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	2
124.50.123.224	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
41.206.63.133	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
196.200.16.202	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
115.139.225.125	Korea, Republic of	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
182.246.30.36	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
218.110.163.110	Japan	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
116.21.203.211	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
41.206.63.131	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
196.200.16.200	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
106.80.129.160	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
121.236.143.72	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
41.206.63.132	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
196.200.16.201	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

02-03-2016-15:04:00 to 02-03-2016-16:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
208.109.97.62	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-03-2016-15:04:00 to 02-03-2016-16:04:00

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	3
2.52.31.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.168.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.96.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.167.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.38.118	147.237.77.170	Israel	maarachot.idf.il	SERVER-APACHE Apache Killer denial of service tool exploit attempt	1
79.176.31.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.93.50.130	147.237.77.235	Korea, Republic of	sviva.idf.il	ET SCAN NMAP -f -sS	1
2.54.49.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.43.246.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.200.30.168	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.3.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.146.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.227.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.220.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.57.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.93.50.130	147.237.77.235	Korea, Republic of	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
5.29.38.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-03-2016-15:04:00 to 02-03-2016-16:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.122.39	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	251
37.26.146.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
109.66.125.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
109.64.48.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
46.19.86.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.147.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
2.52.183.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.181.105.82	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
84.109.74.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
46.19.86.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.97	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	13
62.219.162.91	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
80.246.133.102	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.135.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.54.183.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
80.246.133.102	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.54.45.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
176.13.8.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.61.146	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
78.171.219.75	Turkey	147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	7
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.141.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.135.187	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.79.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.6.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.116.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.219.164	Israel	147.237.76.86	navy.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	5
85.64.111.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.134.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
149.88.229.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
149.88.229.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.147.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.147.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
188.120.148.74	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.19.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.147.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.199	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.147.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

02-03-2016-15:04:00 to 02-03-2016-16:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.193.183	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
109.253.211.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
109.253.211.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
2.54.149.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
84.229.129.248	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
2.54.35.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
185.32.179.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.52.183.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
37.26.148.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
109.253.211.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
2.54.16.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
176.13.11.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
94.199.151.22	United Kingdom	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 94.199.151.22	Block	5
210.157.22.62	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 210.157.22.62	Block	4
46.19.86.187	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
80.246.139.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	3
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
184.75.83.66	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	3
2.54.179.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
109.253.134.232	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.169.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.183.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.19.86.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.131.133	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$61 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
77.127.114.57	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
109.253.196.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$117 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.147.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
37.26.149.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.204.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$8 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
80.246.139.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
213.151.54.142	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
31.168.151.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.121.111.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method [[#29]]:%Ã¹bÂ…Ã”Ã¶Ã»,oCÃ¢Ã…Ãš [[#6]]Â”Â¥Â˜Ã”Ãš[[#29]]U[[#6]][[#17]]ÂŸÃ–4Ã?TxgtJÃ²;-Âº{ÃŒWWÂƒÂš FÃˆÃ¬Ã‚ÂŽÂ™Â”Â„Ã¾u[[#23]]Â¼:[[#4]]Rn~Â† in URL	Block	1
31.210.187.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$60 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.253.141.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.120.125.15		147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$24 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.52.158.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$78 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
80.246.138.130	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$2 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
80.178.201.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
149.88.87.49	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$120 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
70.54.85.73	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/faq.aspx	Block	1
109.66.4.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

02-03-2016-15:04:00 to 02-03-2016-16:04:00

02-03-2016-15:04:00 to 02-03-2016-16:04:00