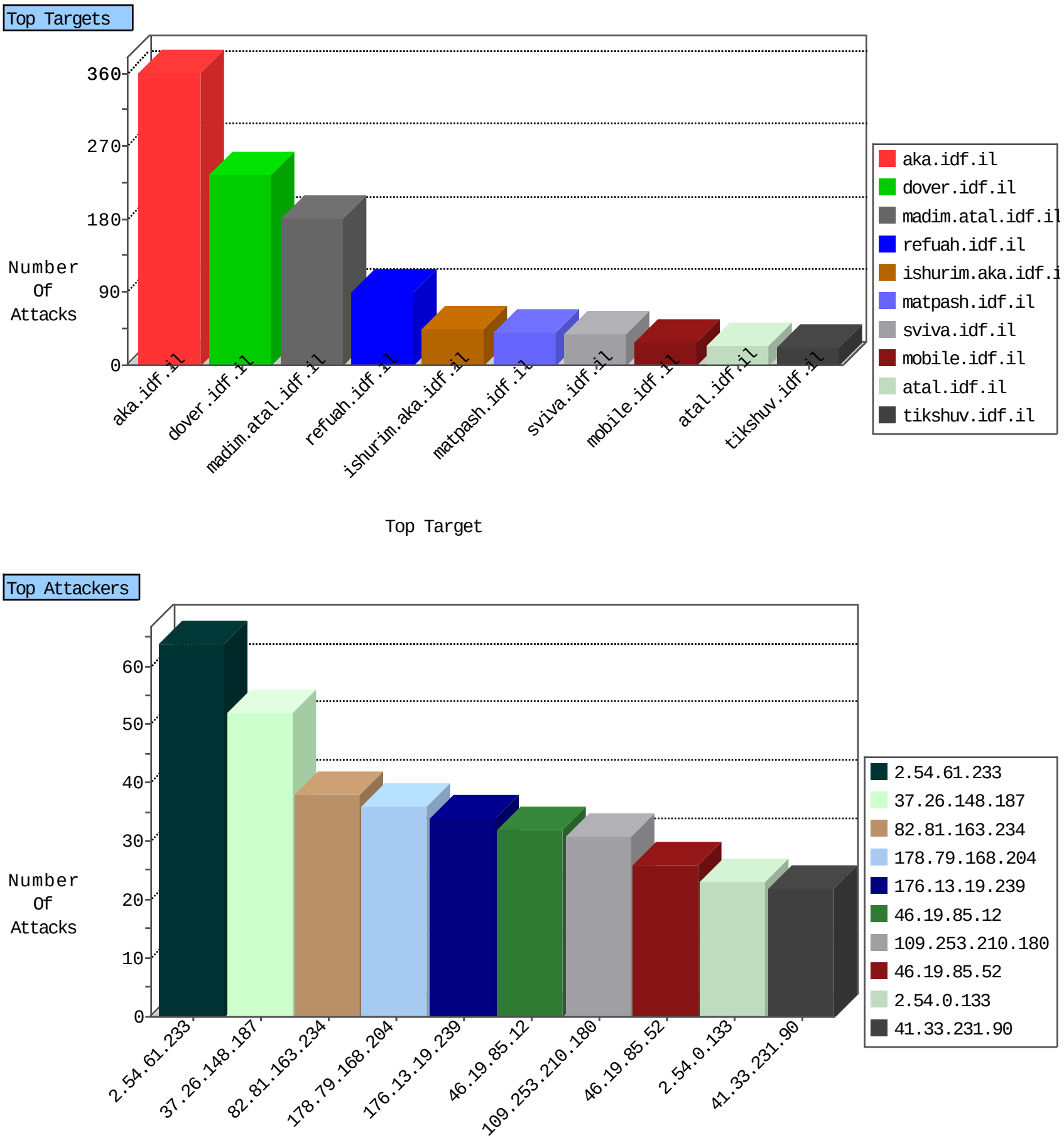
02-10-2016-11:04:07 to 02-10-2016-12:04:07

IDF Under Attack Daily Report



02-10-2016-11:04:07 to 02-10-2016-12:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.215.198.132	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
62.117.59.18	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
77.125.156.31	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.179.25.7	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.64.43.164	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
5.22.129.81	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.94.111.1		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
61.49.45.41	China	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
185.94.111.1		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

02-10-2016-11:04:07 to 02-10-2016-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-10-2016-11:04:07 to 02-10-2016-12:04:07

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	2
2.54.5.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.152.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.241.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.180.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
164.39.11.198	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.6.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.196.49.101	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -f -sS	1
84.108.40.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.211.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.196.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.53.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.79.168.204	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.214.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.196.49.101	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -sS window 2048	1

02-10-2016-11:04:07 to 02-10-2016-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.81.163.234	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
176.13.19.239	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
46.19.85.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
46.19.85.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
2.54.156.227	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
178.79.168.204	United Kingdom	147.237.77.235	sviva.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.107	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
178.79.168.204	United Kingdom	147.237.77.235	sviva.idf.il	drop		drop	10
193.55.99.229	France	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.130.65	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.52.163.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
5.22.134.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.187	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.14.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.170.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.66.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.227.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.96.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.76.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.187	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.148.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.148.187	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
188.120.148.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.140.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
82.145.210.171	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.79.168.204	United Kingdom	147.237.77.235	sviva.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.132.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.20.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
188.247.72.134	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
176.13.20.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.239	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.148.187	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.0.133	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.163.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.192.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.85.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.3.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.148	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.222.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-10-2016-11:04:07 to 02-10-2016-12:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.61.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
109.253.210.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
109.253.145.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
77.125.125.99	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
185.32.179.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
85.64.14.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
80.246.136.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
2.54.0.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
95.35.4.120	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	3
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.4.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
199.203.226.21	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 199.203.226.21	Block	2
176.13.0.63	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.0.63	Block	2
46.19.86.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.63.147	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
149.88.112.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
80.246.133.178	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.133.178	Block	2
2.54.128.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.8.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
31.44.143.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21240-he/idfgdover.aspx&sa=u&ved=0ahukewjx3jg17ezkahwf_a4khtw6c1kqfggjmaa&usg=afqjcnfefno7hnhawhelbeqbtov7rjs7ma	Block	2
192.117.141.177	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
109.253.131.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.4.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
147.235.236.1	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-9481-he/cogat.asp	Block	1
213.151.48.4	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/110435.pdf	Block	1
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.13.19.239	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
93.172.178.199	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
37.26.146.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
162.243.222.171	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 162.243.222.171	Block	1
109.253.142.90	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
62.219.228.23	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
85.93.91.84	Germany	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/×ž×?×™×¨	Block	1
46.19.85.95	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
175.198.148.195	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/<!doctype	Block	1
5.22.134.204	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Malformed URL	Block	1
2.52.7.144	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$0 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
149.78.59.15	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 149.78.59.15 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$61 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.27	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
178.79.168.204	United Kingdom	147.237.77.235	sviva.idf.il	Unauthorized HTTP Method	Block	1
95.35.4.120	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.35.4.120	Block	1
82.81.163.234	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1

02-10-2016-11:04:07 to 02-10-2016-12:04:07