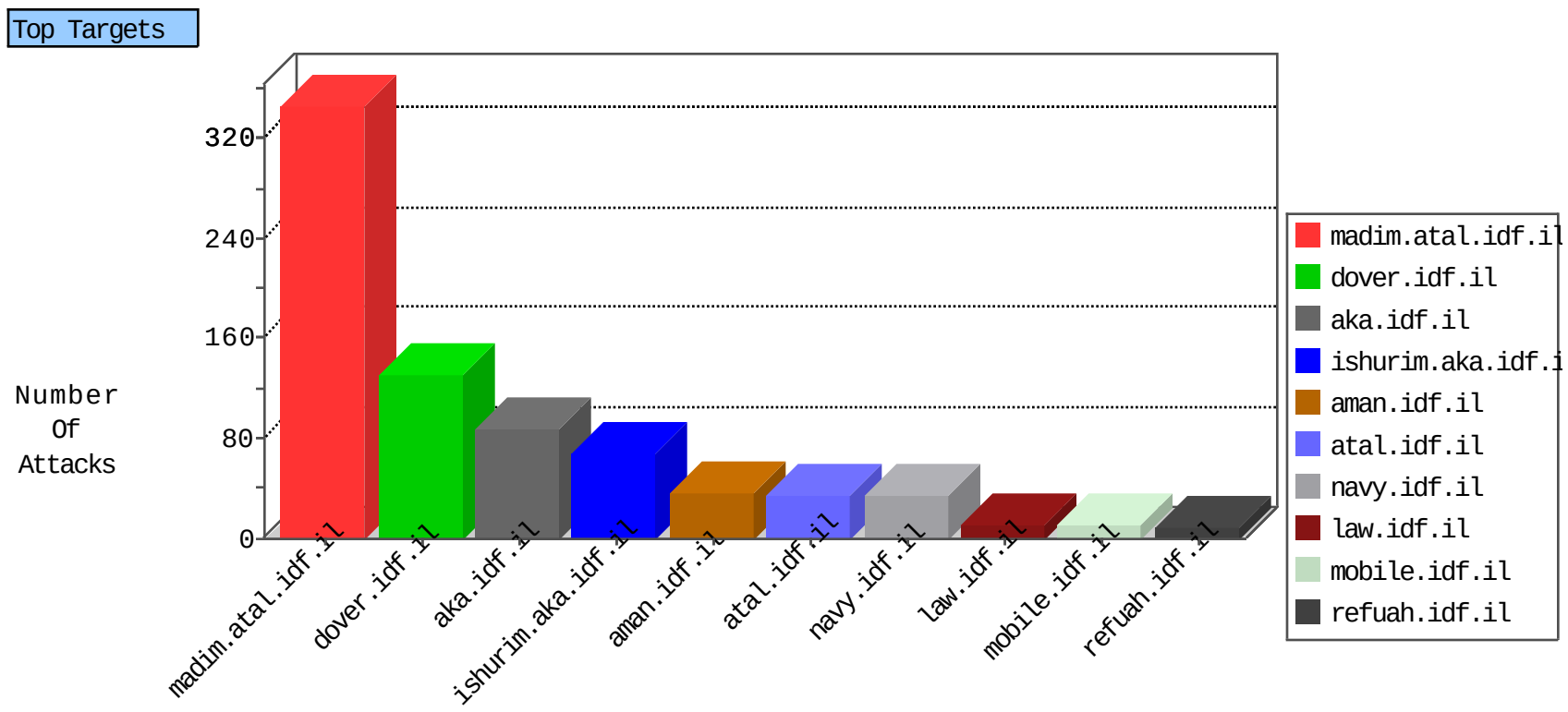
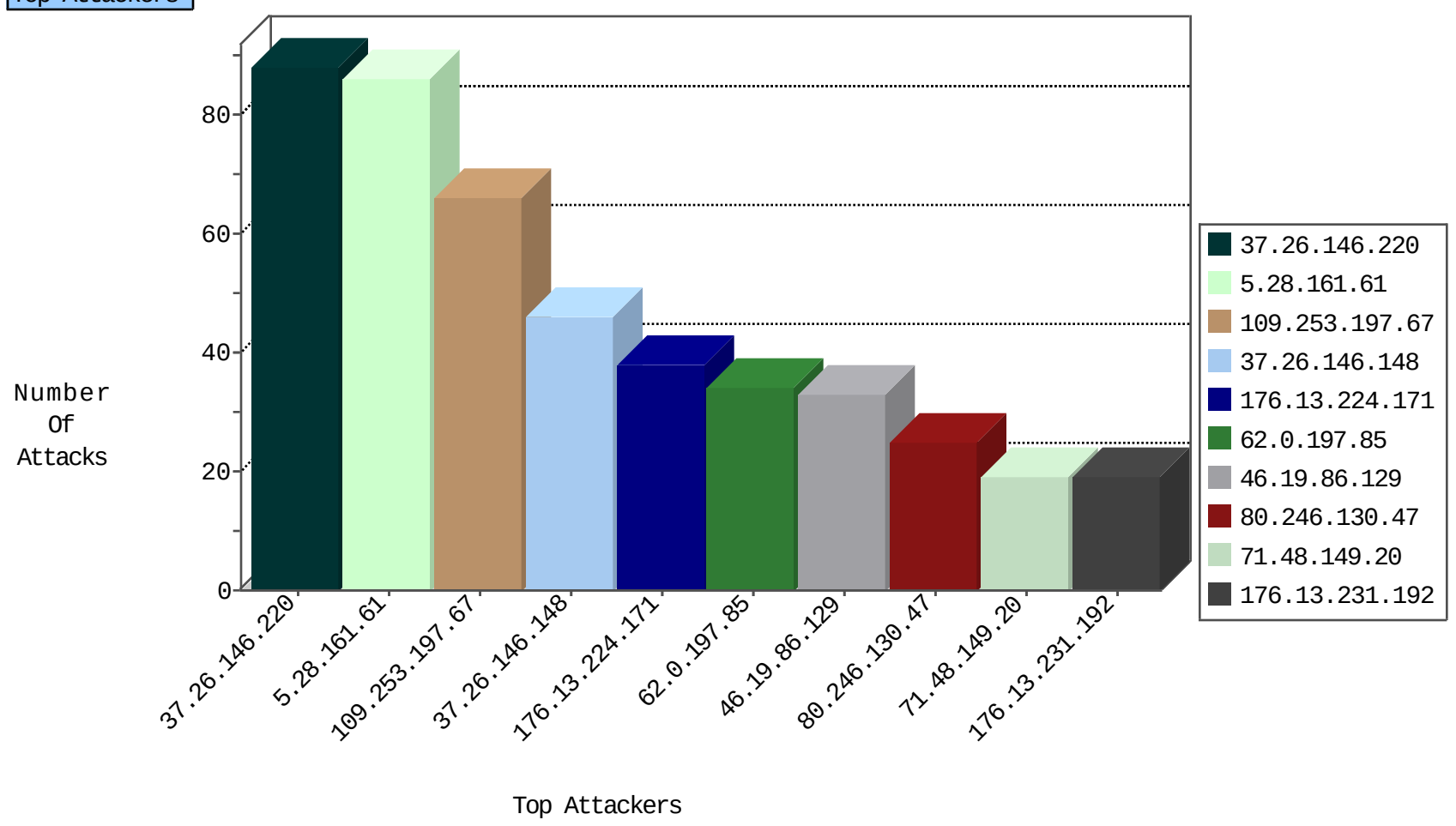
09-05-2016-13:04:03 to 09-05-2016-14:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-05-2016-13:04:03 to 09-05-2016-14:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.224.100	Israel	147.237.72.156	aman.idf.il	L4 Source or Dest Port Zero	drop	4
120.59.83.3	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
209.126.136.2	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
46.19.85.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.82.65.168	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
46.116.172.133	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
62.219.146.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.136.2	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1

09-05-2016-13:04:03 to 09-05-2016-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.68.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

09-05-2016-13:04:03 to 09-05-2016-14:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.178.20.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.106.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.58.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.40.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.245.183.109	147.237.76.200	Indonesia	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
141.226.162.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.187.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.4.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.121.81.33	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
87.69.155.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.169.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.18.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.198.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.6.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.182.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.221.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.52.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.24.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-05-2016-13:04:03 to 09-05-2016-14:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.197.67	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
62.0.197.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
80.246.130.47	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
46.19.86.38	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
71.48.149.20	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.70.57.71	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
62.0.200.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.137	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
41.254.0.131	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.55.30.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.0.205.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
71.48.149.20	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
85.130.219.42	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.0.197.85	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
66.102.9.157	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
109.253.210.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.43.246.250	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
92.70.135.242	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
141.226.218.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
71.48.149.20	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
2.53.44.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.142	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.139.200.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
80.179.114.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.236.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
71.48.149.20	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
109.253.194.187	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
2.53.49.103	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.146.220	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	2
117.194.239.248	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.236.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
71.48.149.20	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
62.0.34.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.231.192	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.102.9.128	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
2.53.161.123	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.64.185.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.56	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.161.123	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
139.162.37.147	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.253.138.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.179.140.133	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

09-05-2016-13:04:03 to 09-05-2016-14:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.28.161.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
37.26.146.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
37.26.146.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
176.13.224.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.19.86.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.231.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
80.246.139.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
80.246.130.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
131.253.27.108	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.53.25.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
62.0.101.97	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.0.101.97	Block	4
31.154.53.142	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	4
109.64.28.212	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
85.64.92.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.237.97.183	France	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
109.253.157.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.53.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
165.225.72.74	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	3
109.66.186.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.92.89	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.64.92.89	Block	2
2.53.142.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.227.91	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	2
85.64.92.89	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
131.253.25.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.229.24.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/undefined	Block	1
213.57.159.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.131	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem	Block	1
77.139.170.107	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
62.219.110.152	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
89.139.186.62	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
212.179.21.199	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/69045.pdf	Block	1
167.220.196.11	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
5.51.131.5	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/	Block	1
194.72.238.241	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
79.176.133.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl80.x in aka.idf.il/main/sachar/payslips.aspx	None	1
155.56.68.217	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/portalmiluim/templates/inner.asp	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.53.32.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.37.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
176.13.12.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl91 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.181.182.195	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
157.55.12.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/1128-he/patzar.aspx	Block	1
37.26.149.146	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1

09-05-2016-13:04:03 to 09-05-2016-14:04:03