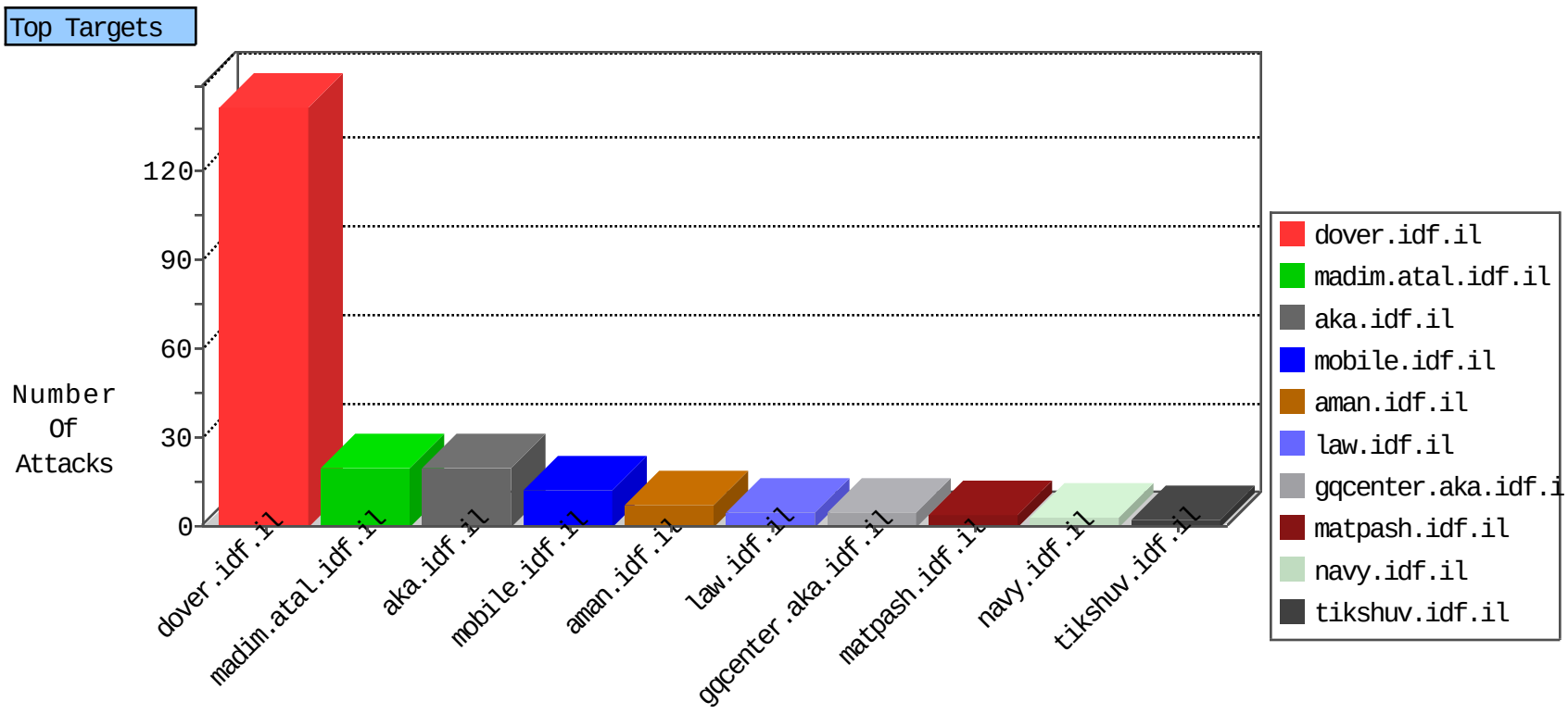
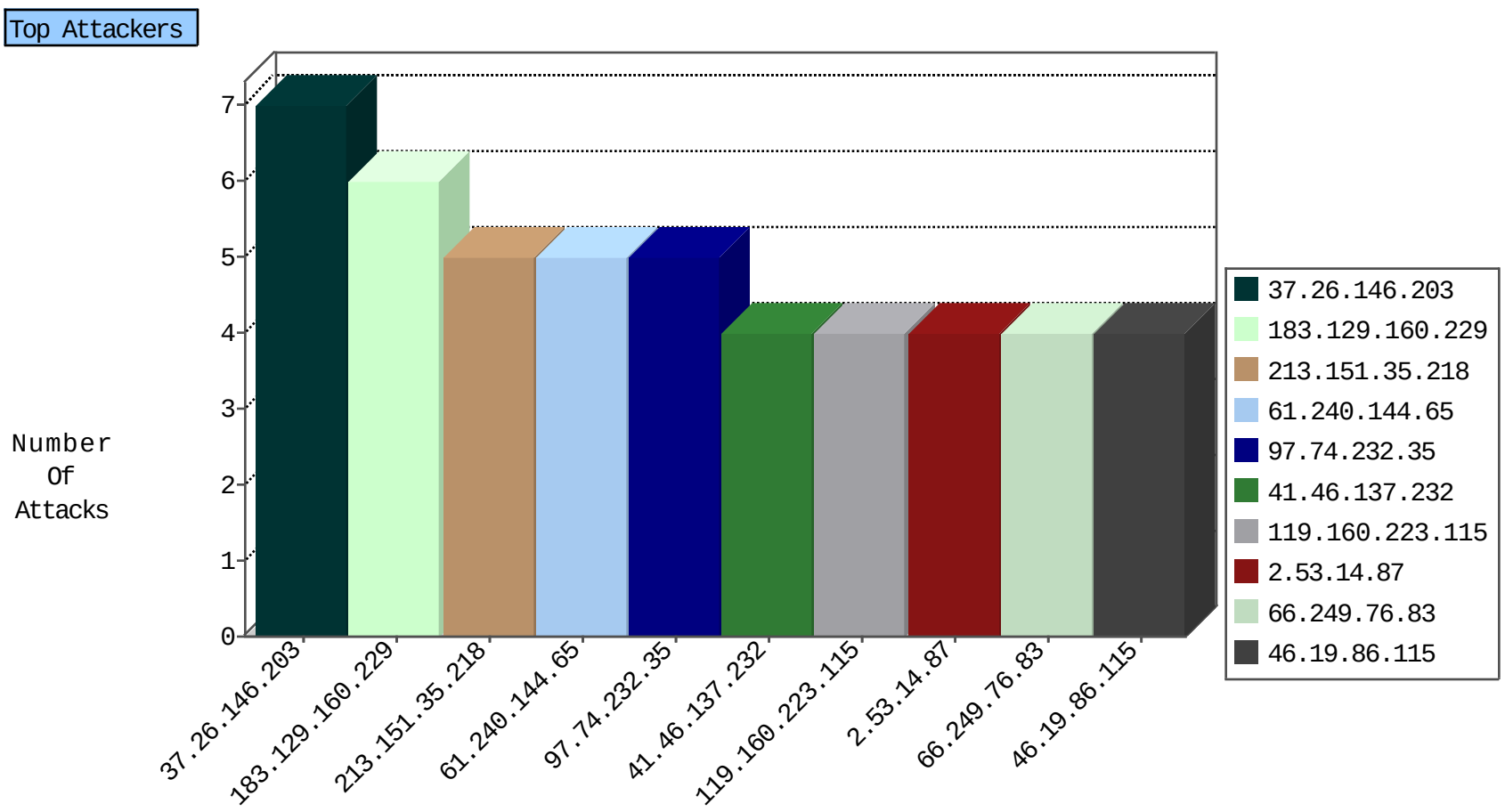
09-01-2016-22:04:02 to 09-01-2016-23:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-01-2016-22:04:02 to 09-01-2016-23:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
182.212.63.82	Korea, Republic of	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
141.226.218.59	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.34	yohalan.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
185.128.40.162	Switzerland	147.237.76.44	e.refuah.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

09-01-2016-22:04:02 to 09-01-2016-23:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-01-2016-22:04:02 to 09-01-2016-23:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.65.148.144	147.237.72.166	Israel	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
146.200.66.247	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
109.60.153.178	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
106.51.226.59	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
185.93.185.10	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
97.74.232.35	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
97.74.232.35	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
119.160.223.115	147.237.76.148	Thailand	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.176	China	matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
119.160.223.115	147.237.72.156	Thailand	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
116.12.175.233	147.237.77.74	Singapore	law.idf.il	ET SCAN NMAP -sS window 4096	1
106.51.226.59	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
193.201.225.149	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
97.74.232.35	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
97.74.232.35	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
97.74.232.35	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.235	China	sviva.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
119.160.223.115	147.237.76.86	Thailand	navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
119.160.223.115	147.237.0.19	Thailand	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
116.12.175.233	147.237.77.74	Singapore	law.idf.il	ET SCAN NMAP -sS window 1024	1

09-01-2016-22:04:02 to 09-01-2016-23:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.46.137.232	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.101	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
176.228.43.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.130.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
1.22.102.195	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
146.185.56.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
187.90.50.116	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
39.113.34.49	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.209.104.59	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
191.206.17.73	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
1.108.192.54	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
61.240.144.65	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
128.232.110.28	United Kingdom	147.237.0.35	akaws.idf.il	drop		drop	1
188.69.225.24	Lithuania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
47.59.163.96	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
116.120.65.1	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
221.138.177.104	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.210.151.32	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
178.139.78.26	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.4.36.54	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.208.254.80	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
191.195.7.103	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
58.124.212.65	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
121.124.241.7	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
47.59.44.70	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
179.112.190.71	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
218.237.125.85	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
39.116.83.96	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.209.184.93	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
177.196.123.87	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
205.155.38.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
1.108.194.104	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.28	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
189.66.78.12	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
47.59.169.4	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
117.233.168.55	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
45.210.171.14	Ghana	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.210.172.116	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
178.139.84.103	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
31.216.208.86	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.209.18.81	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1

09-01-2016-22:04:02 to 09-01-2016-23:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
213.151.35.218	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	5
84.94.66.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.53.14.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
213.151.55.238	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
2.53.142.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.69.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
2.55.36.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.23.169	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
46.19.86.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.147.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
79.182.1.224	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
212.199.57.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
81.218.207.47	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/maslulimlist.aspx	Block	2
109.253.208.106	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
66.249.64.234	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/112981.pdf	Block	1
176.58.92.217	United Kingdom	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/index.php	Block	1
46.19.86.115	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
46.117.69.104	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מאיר שחמון.aspx	Block	1
109.253.208.187	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/matash/login/	Block	1
79.180.37.240	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.240	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/watercrafts.aspx	Block	1
185.3.147.141	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
46.19.86.115	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
84.108.213.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19754-he/dover.aspx	Block	1
46.120.220.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
128.232.110.28	United Kingdom	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for 147.237.77.235/	Block	1
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.19.86.115	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=10d686b9451d0c1b.1472756945.1.1472756945.1472756945.;	Block	1
95.86.102.196	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
157.55.39.252	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
5.189.103.54	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.75.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19163-he/dover.aspx	Block	1
46.19.86.115	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method .8afc=%5B%22%22%2C%22%22%2C1472756945%2C%22android-app%3A%2F%2Fcom.google.android.googlequicksearchbox%22%5D; in URL _pk_id.20.8afc=10d686b9451d0c1b.1472756945.1.1472756945.1472756945.	Block	1
2.53.49.100	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.65.95.49	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
77.125.8.9	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.102.9.13	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
176.58.92.217	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/index.php	Block	1
83.130.76.197	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1

09-01-2016-22:04:02 to 09-01-2016-23:04:02