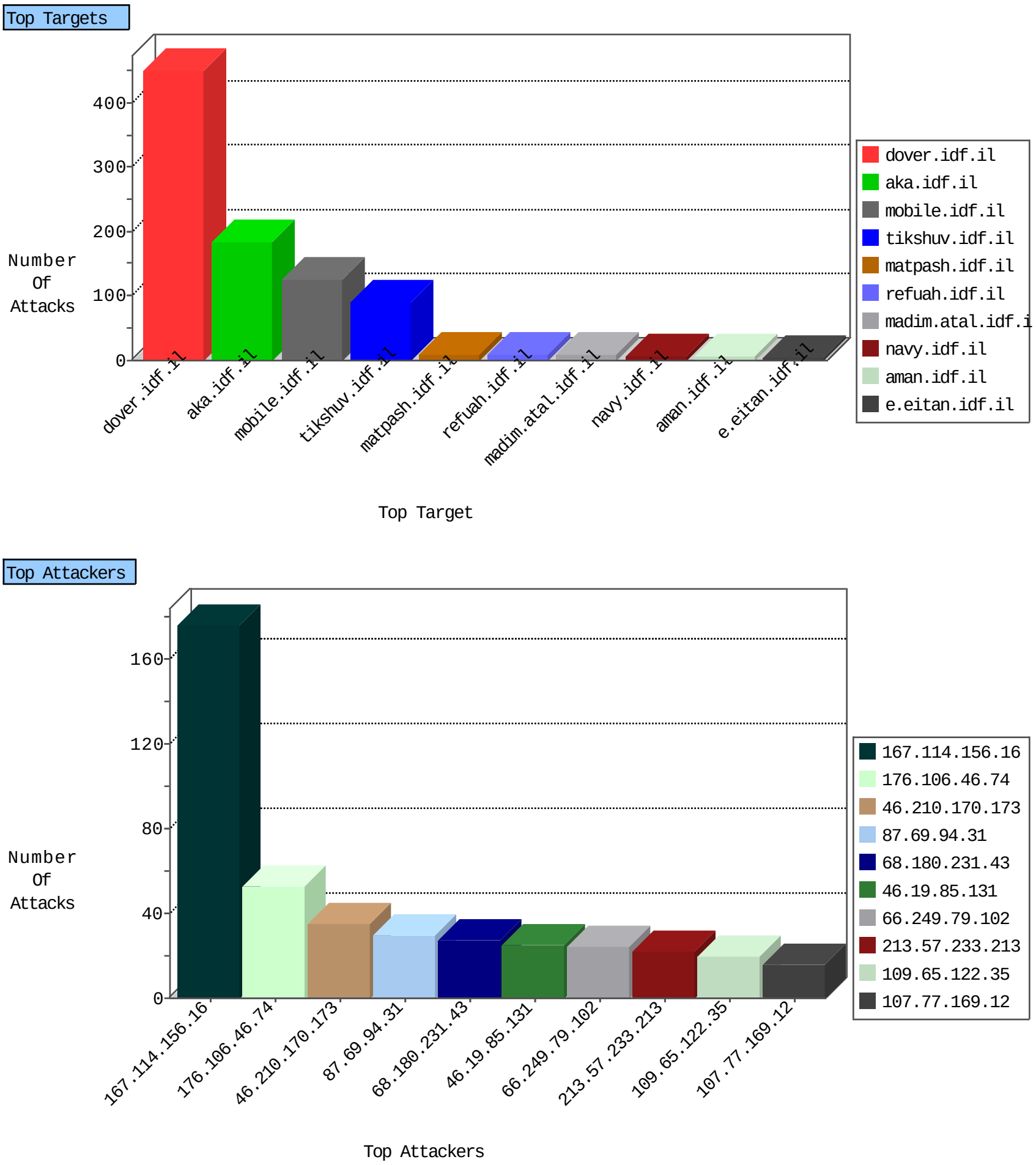
04-30-2016-11:04:05 to 04-30-2016-12:04:05

IDF Under Attack Daily Report



04-30-2016-11:04:05 to 04-30-2016-12:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7213
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1025
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
78.31.67.9	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

04-30-2016-11:04:05 to 04-30-2016-12:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-30-2016-11:04:05 to 04-30-2016-12:04:05

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	4
104.219.238.10	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 1024	1
85.214.134.155	147.237.76.177	Germany	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.79.18	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
119.10.114.32	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
119.10.114.32	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
107.158.255.194	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
107.158.255.194	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 4096	1
85.214.134.155	147.237.76.177	Germany	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
85.214.134.155	147.237.76.177	Germany	ncore.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.0.19	United States	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
119.10.114.32	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
107.158.255.194	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1

04-30-2016-11:04:05 to 04-30-2016-12:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.i	drop	First packet isn't SYN	drop	52
46.210.170.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
87.69.94.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
46.19.85.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.65.122.35	Israel	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
107.77.169.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
213.57.233.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
87.71.6.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.212.110.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.29.164.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.15.190.222	Slovenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.47	United States	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.35.131.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
188.120.154.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
95.91.215.113	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
85.64.85.87	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.116.26.122	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
85.64.85.87	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
94.73.150.148	Turkey	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
109.253.216.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.188.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
162.156.124.156	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.65.5.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.181.227.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.154.52	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.5.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.142.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.160.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-30-2016-11:04:05 to 04-30-2016-12:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.108.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.81.108.113	Block	9
87.69.94.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
213.57.233.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
46.210.170.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
2.53.44.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
82.81.108.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ge...04&docid=73994	Block	2
31.210.186.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.122.35	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation phrase in www.tikshuv.idf.il/modules/forums/searchresults.aspx	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.124.7.38	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
184.105.247.196	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.79.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
60.29.153.13	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
17.142.159.155	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/apple-app-site-association	Block	1
109.64.96.167	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
77.127.187.99	Israel	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
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=87a8a13887d9646d.1458597128.2.1462006466.1462006466.;	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
66.249.66.17	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1094-en/hamaz.aspx	Block	1
79.181.198.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/ctl00_ctl00_cphmain_cphsachar_divpersonalquestionscontent	Block	1
66.249.66.185	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/sitemap/sitemap.aspx	Block	1
207.46.13.40	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 5B%22%22%2C%22%22%2C1462006466%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; in URL _pk_id.20.8afc=87a8a13887d9646d.1458597128.2.1462006466.1462006466.	Block	1
87.69.113.19	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
66.249.66.50	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/tizmoret/klali/default.asp	Block	1
157.55.39.18	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
79.181.198.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __LASTFOCUS in www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	None	1
66.249.78.27	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
207.46.13.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover...	Block	1
87.69.113.19	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
184.105.139.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.79.18	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
52.13.24.133	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
87.71.6.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

04-30-2016-11:04:05 to 04-30-2016-12:04:05