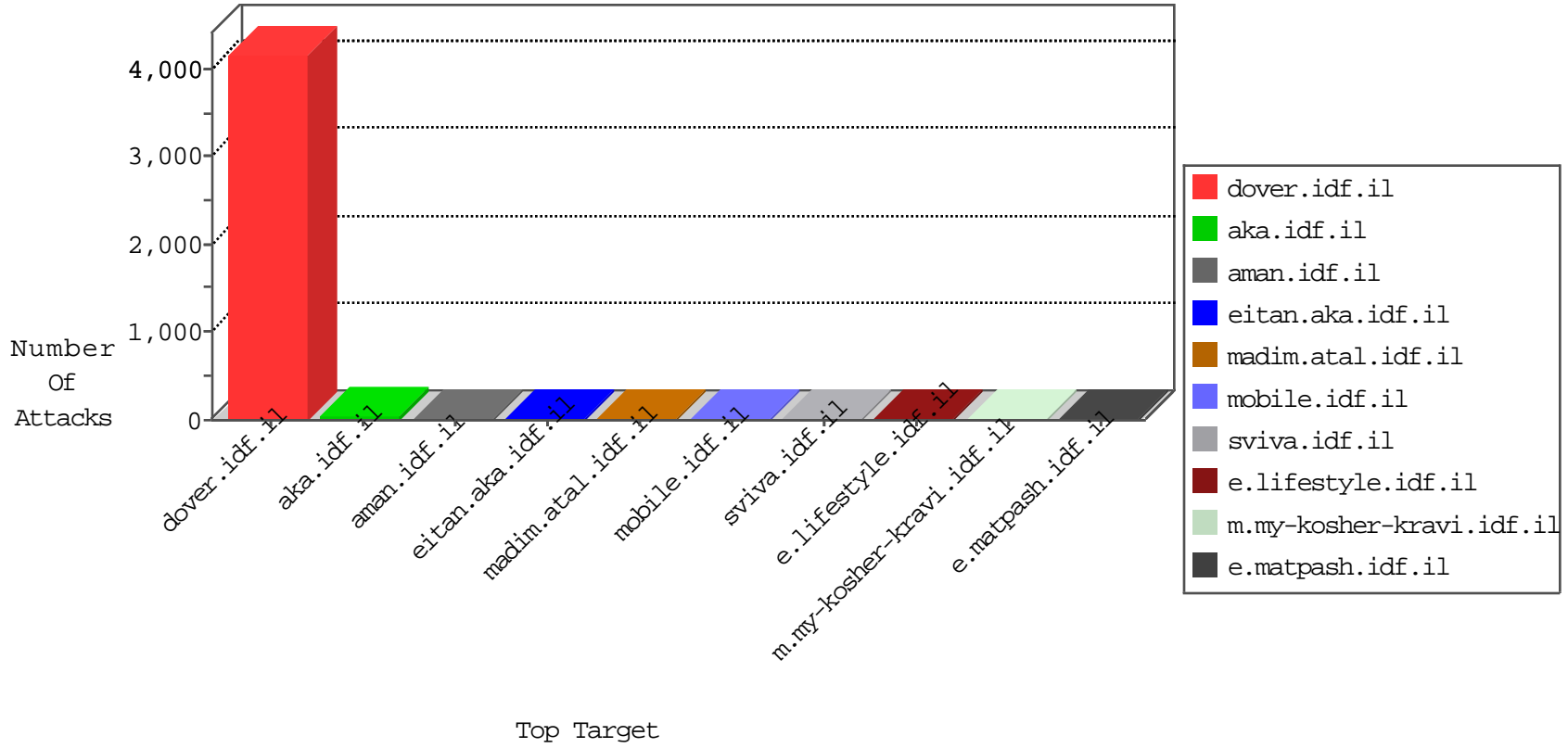


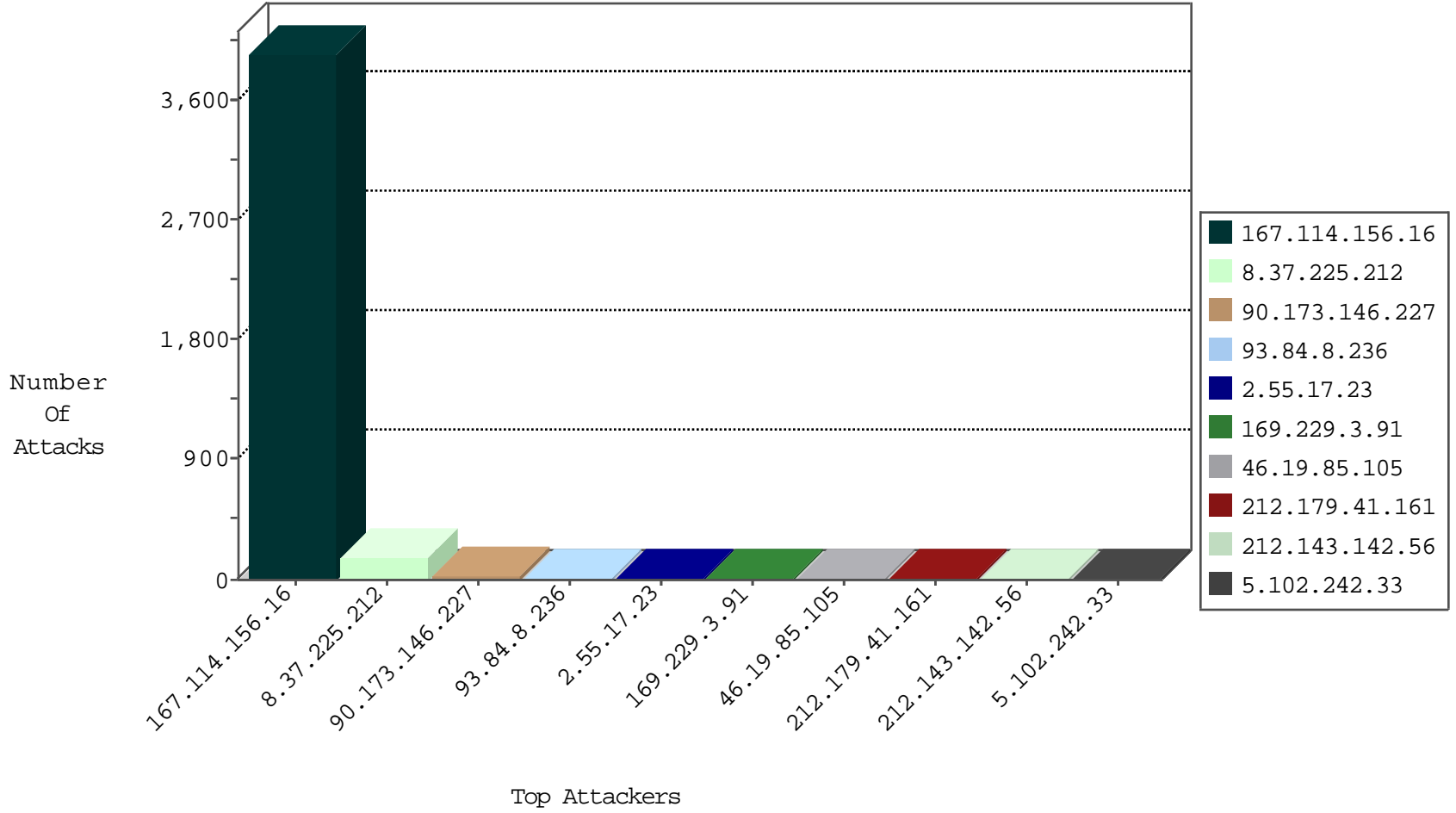
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	Block_Ip_Web_In	drop	3943
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
8.37.225.212	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
8.37.225.212	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
184.105.139.116	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.108	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
90.173.146.227	147.237.76.30	Spain	himush.idf.il	ET SCAN Potential SSH Scan	2
90.173.146.227	147.237.77.19	Spain	law-forum.idf.il	ET SCAN Potential SSH Scan	2
90.173.146.227	147.237.76.198	Spain	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
90.173.146.227	147.237.76.148	Spain	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
106.186.113.67	147.237.77.235	Japan	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
90.173.146.227	147.237.76.39	Spain	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.77.243	Spain	mobile.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.77.227	Spain	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.72.166	Spain	aka.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.77.179	Spain	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
89.216.119.94	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
90.173.146.227	147.237.77.121	Spain	e.navy.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.0.16	Latvia	ny-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.5.147	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
90.173.146.227	147.237.76.199	Spain	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
90.173.146.227	147.237.76.177	Spain	ncore.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -f -sS	1
90.173.146.227	147.237.76.44	Spain	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
106.184.2.29	147.237.72.166	Japan	aka.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.76.34	Spain	yohalan.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.77.235	Spain	sviva.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.72.217	Spain	e.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.77.212	Spain	e.dover.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.72.156	Spain	aman.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.77.178	Spain	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
89.216.119.94	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.235	United States	sviva.idf.il	ET DROP Dshield Block Listed Source	1
90.173.146.227	147.237.77.74	Spain	law.idf.il	ET SCAN Potential SSH Scan	1
90.173.146.227	147.237.76.200	Spain	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	155
2.55.17.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.105	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.179.41.161	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.242.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.146.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.27.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.79.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.112.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.24	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
67.243.55.213	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
176.228.140.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.225.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
31.210.188.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
159.226.95.66	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
73.244.90.178	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.235	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illegal start line in request	monitor	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.60	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.72.70.2	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
132.252.173.4	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.10	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
201.247.3.126	El Salvador	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
149.88.135.53	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
37.26.147.138	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
132.252.173.4	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.10	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
158.255.5.147	Russian Federation	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.7.61.94	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.104	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.38.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.211	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.32	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
158.255.5.147	Russian Federation	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
73.7.61.94	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.116	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.193.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.84.8.236	Belarus	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
93.84.8.236	Belarus	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.84.8.236	Block	5
2.55.16.103	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
217.199.187.68	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 217.199.187.68	Block	3
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
220.255.148.148	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
109.65.224.185	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
58.100.11.222	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
203.127.96.252	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
73.251.139.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
217.199.187.68	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar	Block	1
207.46.13.155	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
184.105.139.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.66.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
207.46.13.176	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method s=5715a8b05006d423000 in URL	Block	1
192.3.2.27	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-en/dover.aspx	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
213.8.204.13	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
93.84.8.236	Belarus	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
58.100.11.222	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	1
203.127.58.237	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1