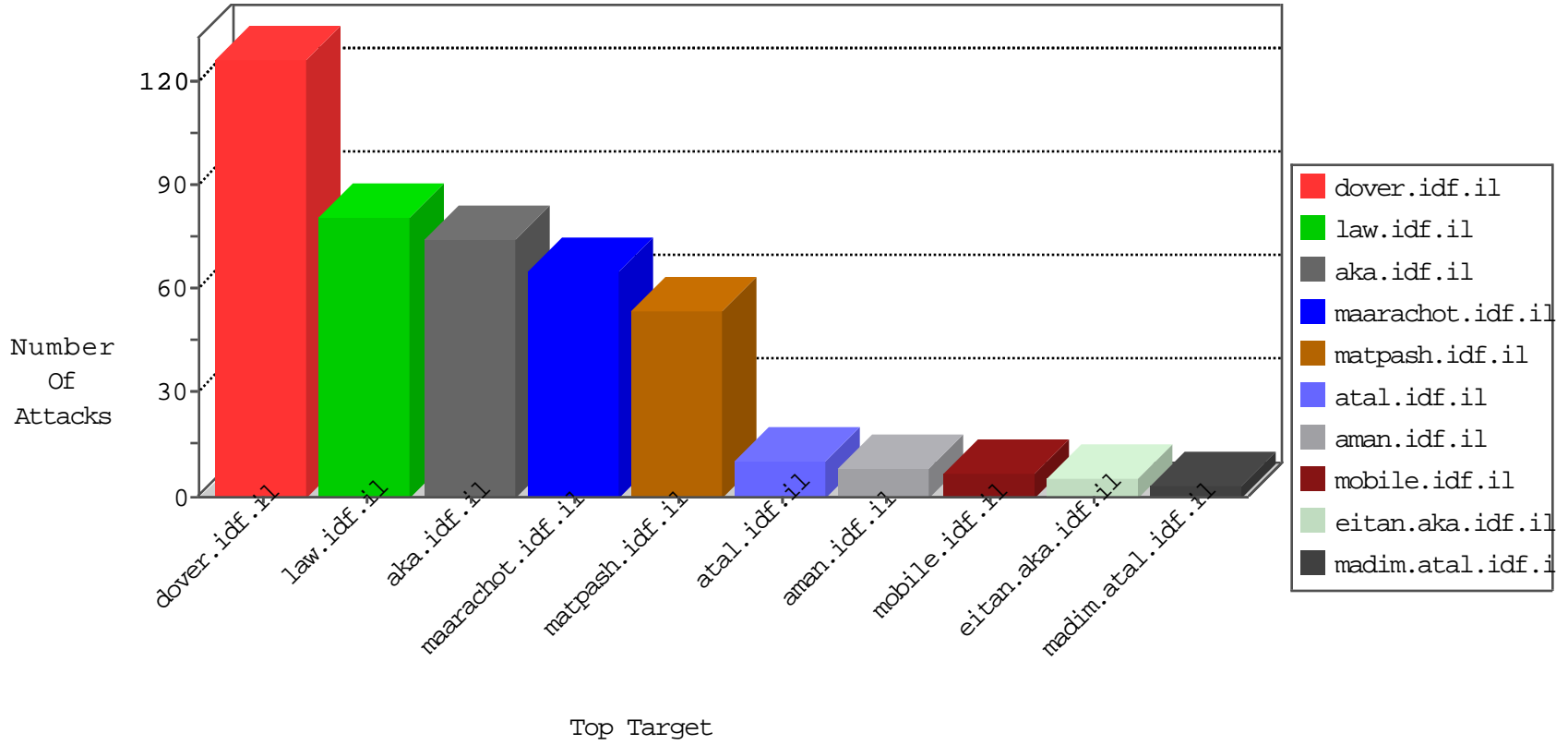


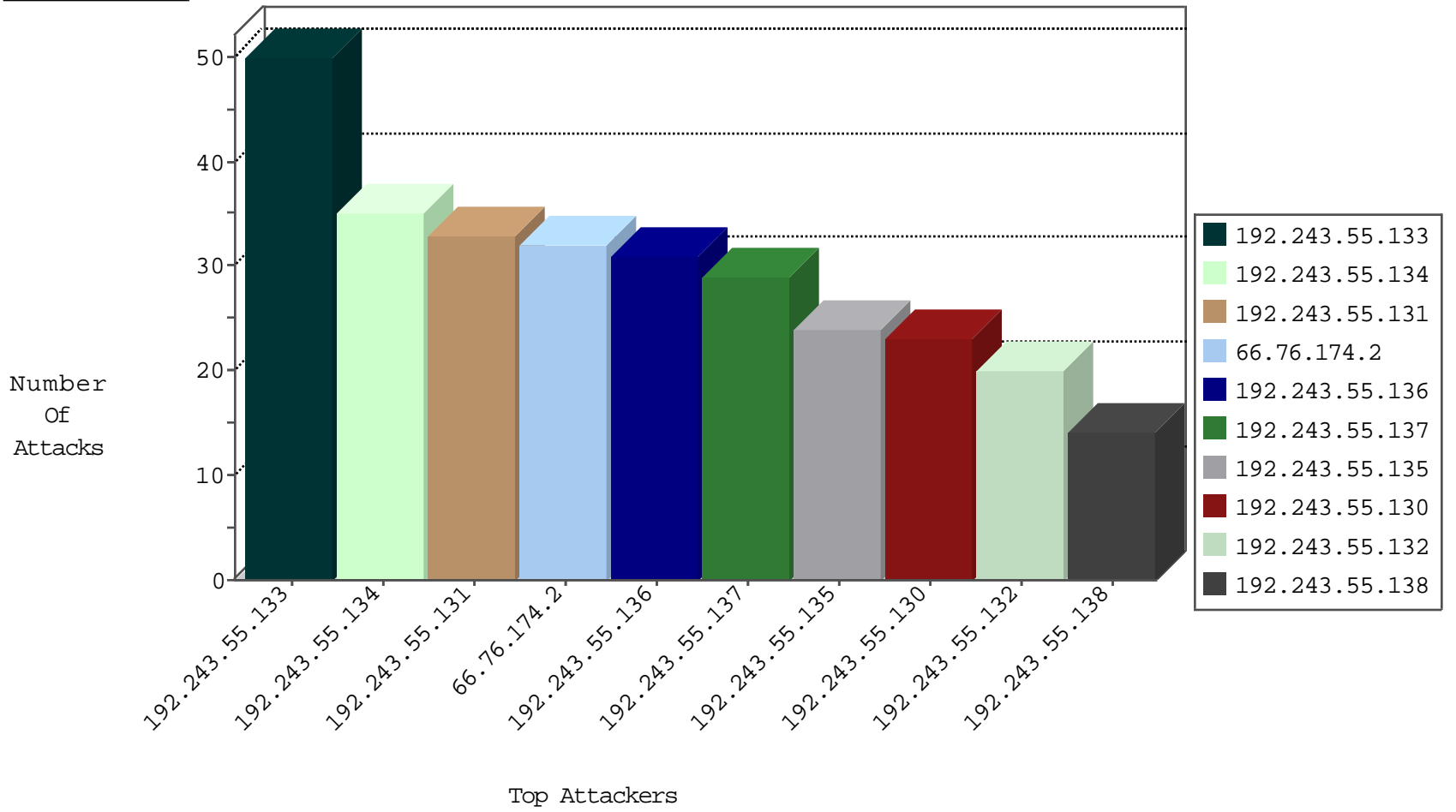
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
117.205.135.56	India	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.40	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
97.99.154.153	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
218.57.11.7	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
141.255.164.234	Switzerland	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
141.255.164.234	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
23.228.107.104	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
141.255.164.234	Switzerland	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
97.99.154.153	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
117.205.135.56	India	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
97.99.154.153	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
210.195.135.235	Malaysia	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.76.174.2	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
61.135.189.69	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.94.63	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.76.174.2	United States	147.237.72.166	aka.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.i	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.94.89	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.94.130	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	1
203.125.85.238	Singapore	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
37.187.95.12	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.76.174.2	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	24
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
5.39.222.253	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.234	147.237.76.148	Switzerland	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
52.87.243.150	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
37.1.209.203	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.235	Canada	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
37.1.209.203	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.230.86.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.133	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.46.41.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.131	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.133.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	Dominica	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.134	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence		monitor	4
46.19.85.4	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.122.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.136	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.131	Dominica	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.120.125.11		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.141	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.131	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
84.228.213.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.13.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.4	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.34.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.137	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.178.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.17.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.0.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15665-en/dover.aspx	Block	1
173.55.77.252	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
40.77.167.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
192.243.55.133	Dominica	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	1
84.108.88.60	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
217.23.39.106	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
174.61.16.52	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/default.aspx	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/14001112010.aspx	Block	1
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhlytayltawms5kb2m=&infocenteritem=true	Block	1
87.139.80.210	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.142.68.1	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
176.13.7.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
87.139.94.177	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.142.68.1	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/kkkkkkk=cd078036kkkkkk_kk_cd078036	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/shared/usercontrols/headerupper/	Block	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19122-en/dover.aspx http://startowy.com/dodajlink.html	Block	1
99.238.9.59	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
185.82.200.91		147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
84.108.88.60	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1