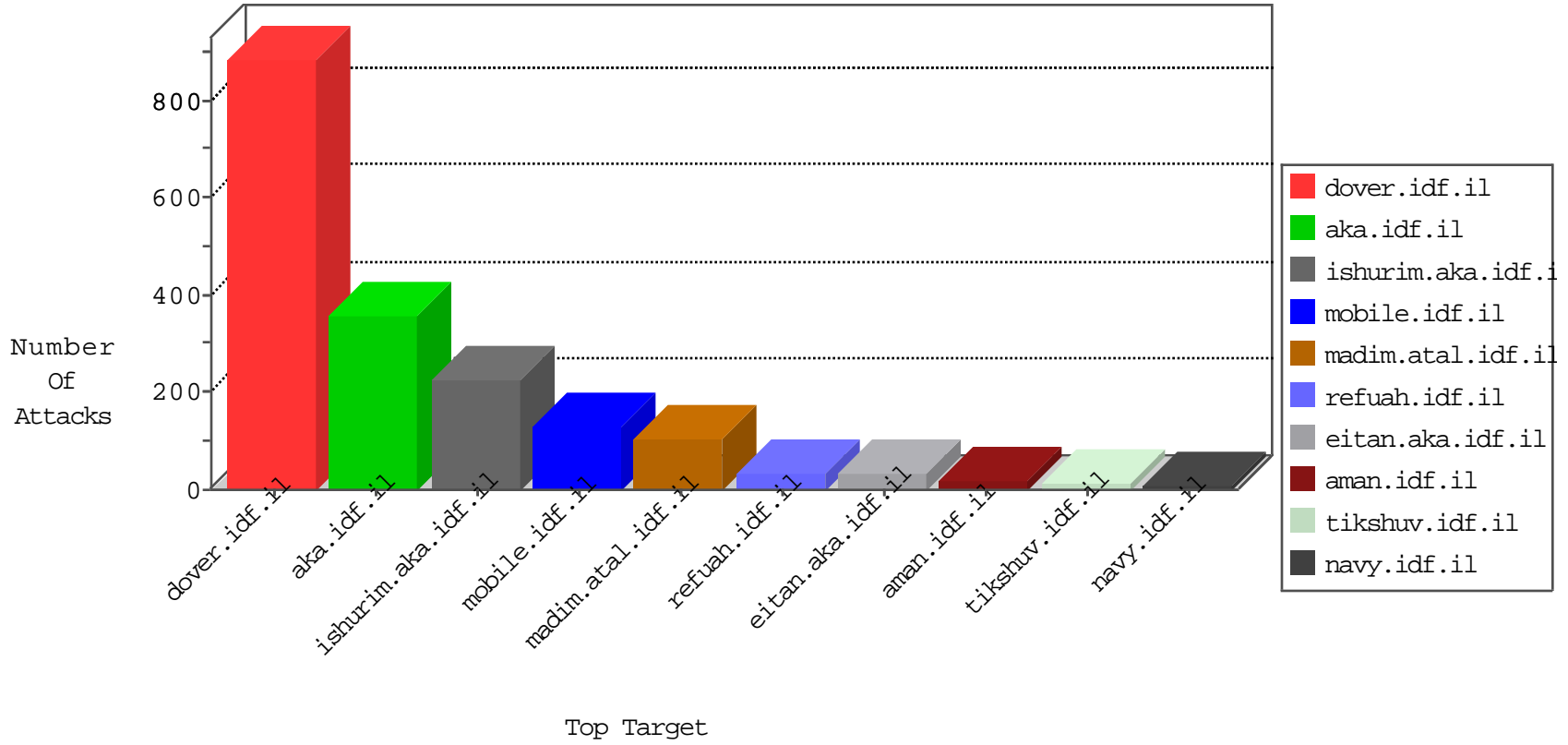


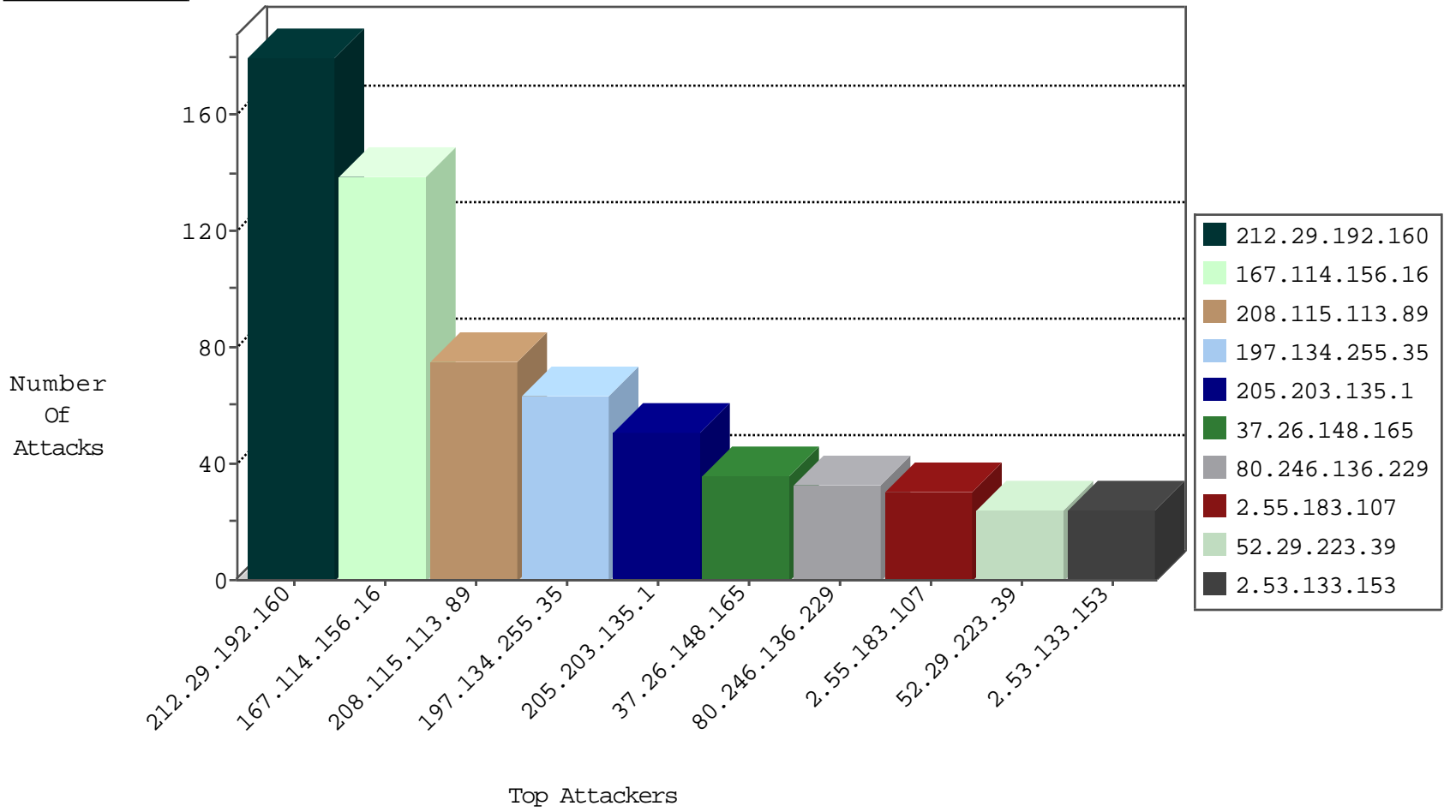
# IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	4747
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2465
85.64.60.195	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	295
81.218.251.251	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
193.254.206.6	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
10.33.252.43		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
123.151.42.61	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Udp	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	2
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
138.134.102.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.227.71.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.61.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.28.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
138.134.102.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.53.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.29.192.160	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
197.134.255.35	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
37.26.148.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.55.183.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
141.0.14.72	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
86.27.79.207	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
109.253.207.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.179.79.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.41.233.139	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
80.246.136.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
95.35.209.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.0.96	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.116.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.88.106.140	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
86.129.200.105	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.80	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.164.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.41.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.192.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.127.129	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.120.154.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.168.231	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.95.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.222.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.53.143.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.95.21.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.46.39.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.78.138.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
2.53.133.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.53.20.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
109.253.207.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
2.55.139.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.55.183.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
95.35.209.68	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
147.236.232.252	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 147.236.232.252	Block	4
147.235.185.74	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
46.19.86.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.53.169.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.90.146	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	3
131.253.25.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.176.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.0.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.135.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.175.192	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.64.171.98	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
147.236.232.252	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 147.236.232.252	Block	2
213.151.43.223	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 213.151.43.223	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.151.43.223	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	2
2.53.6.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.0.68	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.67.175.183	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 109.67.175.183	Block	2
147.236.232.252	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
94.45.188.11	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
212.199.34.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$cb14225959 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
147.236.232.252	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 147.236.232.252	Block	1
46.210.177.43	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
2.55.52.57	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
217.69.133.243	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/smalim/html/4.asp	Block	1
2.53.25.147	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
176.13.9.105	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
84.111.216.11	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
147.236.232.252	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 147.236.232.252	Block	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.147.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.204.36	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	1
151.80.31.153	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1