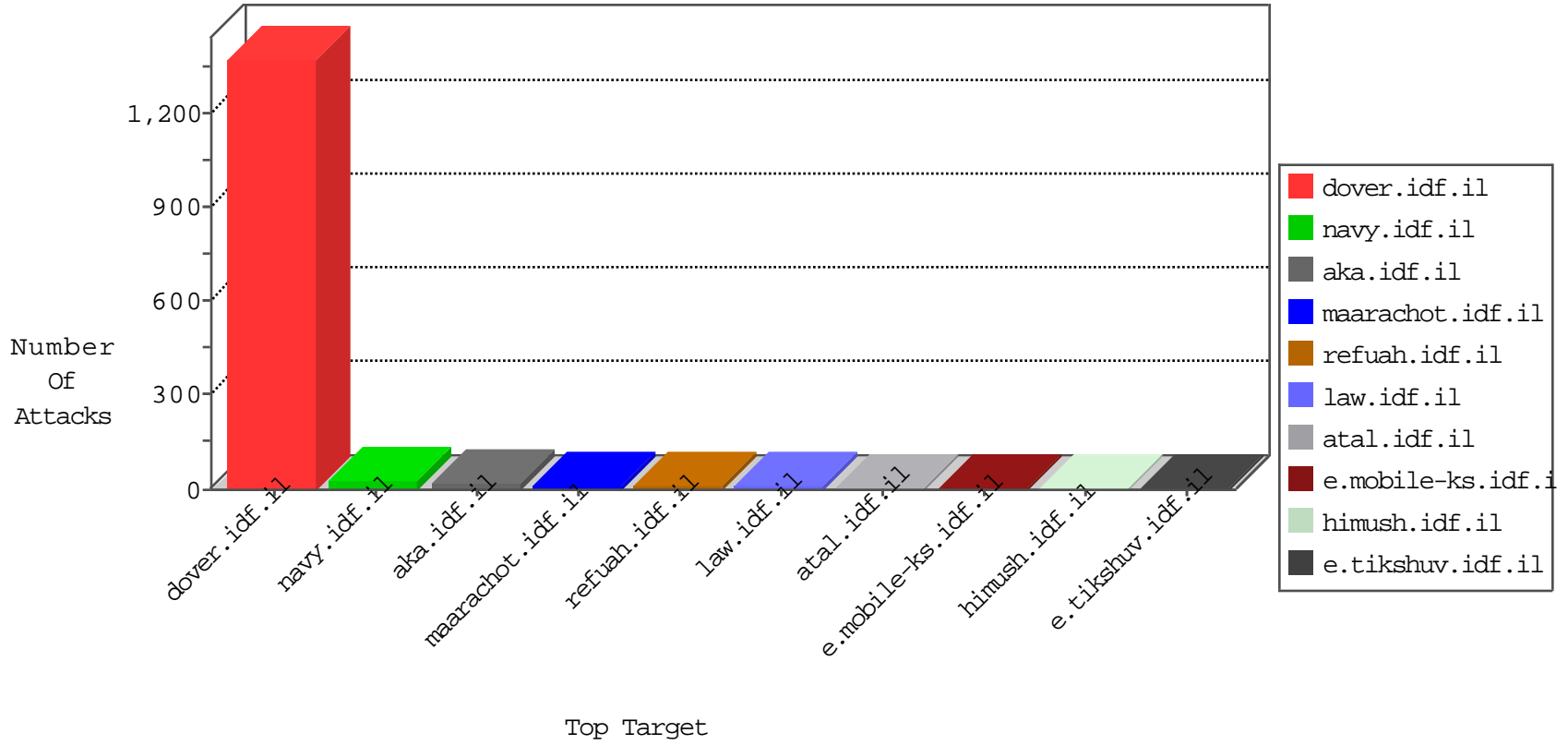
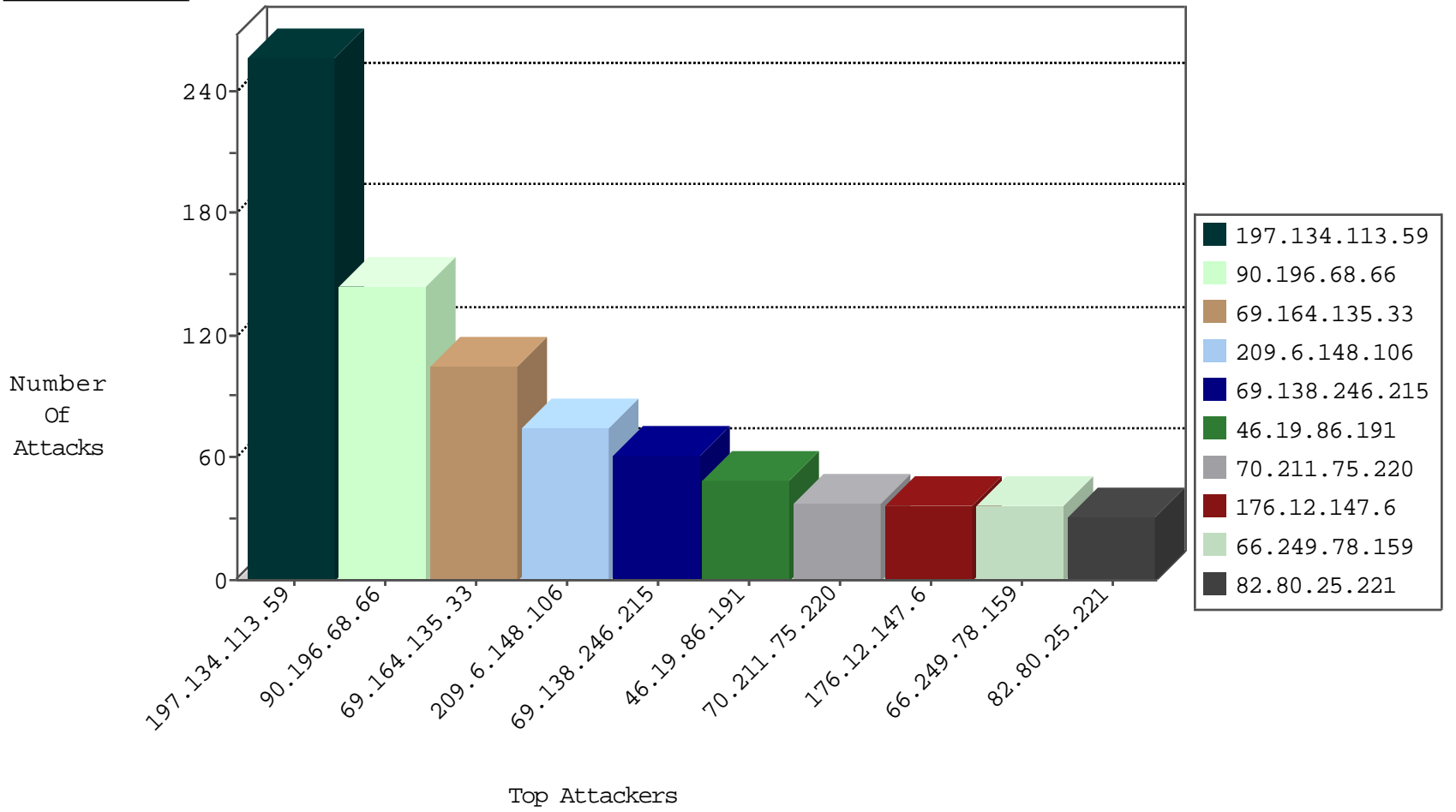




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.179	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	1040
220.181.108.84	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	101
220.181.108.166	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	63
82.145.219.142	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
58.72.58.45	Korea, Republic of	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	26
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
89.139.173.79	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
46.116.193.10	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	29
66.249.67.41	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl IWP with fake user agent	6
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.168	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -f -sS	1
81.200.91.2	Russian Federation	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243		147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
81.200.91.2	Russian Federation	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
197.134.113.59	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	255
90.196.68.66	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	144
69.164.135.33	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	105
209.6.148.106	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	75
69.138.246.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
46.19.86.191	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
70.211.75.220	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
176.12.147.6	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
68.187.129.181	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
220.213.51.77	Japan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
190.167.187.187	Dominican Republic	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
76.23.129.129	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
66.249.64.76	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
208.54.86.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
105.34.241.129		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
23.117.9.93	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
176.12.149.112	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.64.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
37.142.109.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
157.55.39.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.46.13.35	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
81.218.176.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
68.180.228.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.46.13.35	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
45.36.22.74		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
14.201.28.100	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
76.98.34.153	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
176.12.150.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
199.30.25.113	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
74.102.14.238	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
107.77.89.26	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.64.72	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
173.252.88.183	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
70.29.38.165	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.78.109	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
174.89.234.171	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	7
157.55.39.14	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.14	Block	3
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
93.233.31.234	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	2
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.59	Block	2
157.55.39.13	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.13	Block	2
197.134.113.59	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	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
178.33.160.252	Spain	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
109.253.129.88	Israel	147.237.72.166	aka.idf.il	Unknown Parameter [[#2]] in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.71	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/undefined	Block	1
157.55.39.14	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
66.249.65.153	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
180.76.4.211	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
113.29.153.66	Korea, Republic of	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/earth.stm	Block	1
157.55.39.16	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//	Block	1
95.173.171.224	Turkey	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/xæx>x^x'x" x"xžxæx?x"	Block	1
37.142.84.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
183.91.14.219	Vietnam	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
69.30.240.46	United States	147.237.72.167	ishurim.aka.idf.il	Illegal HTTP Version	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/megurim/news/	None	1
157.55.39.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
101.110.183.64	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
188.138.17.205	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
157.55.39.13	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/70069.jpg	Block	1
70.29.38.165	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/join	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/portalmilium/templates/www.behazdaa.org	Block	1
109.253.129.88	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name [[#2]] in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	Block	1
67.231.16.42	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.64.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/mobile/	Block	1
66.249.64.64	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1