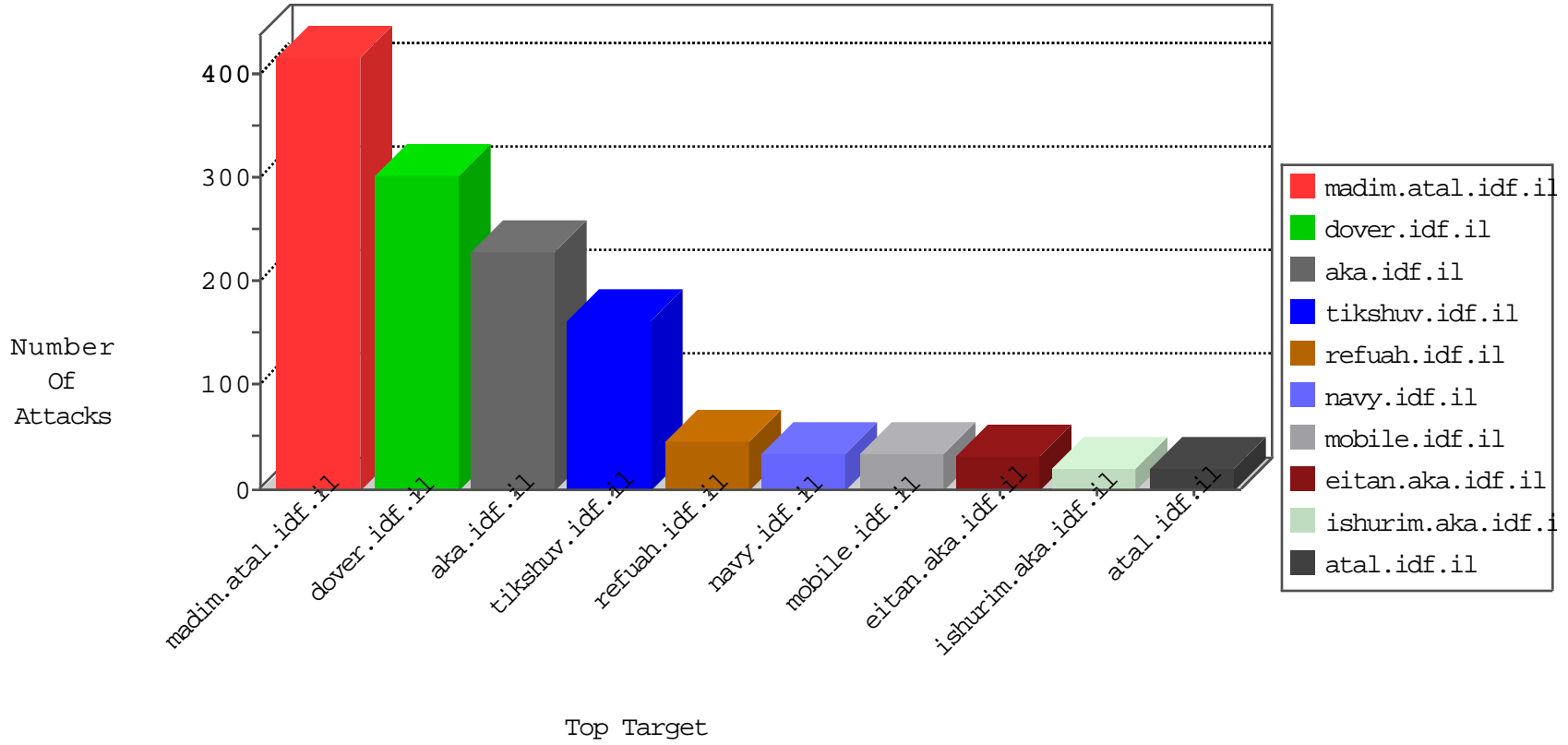


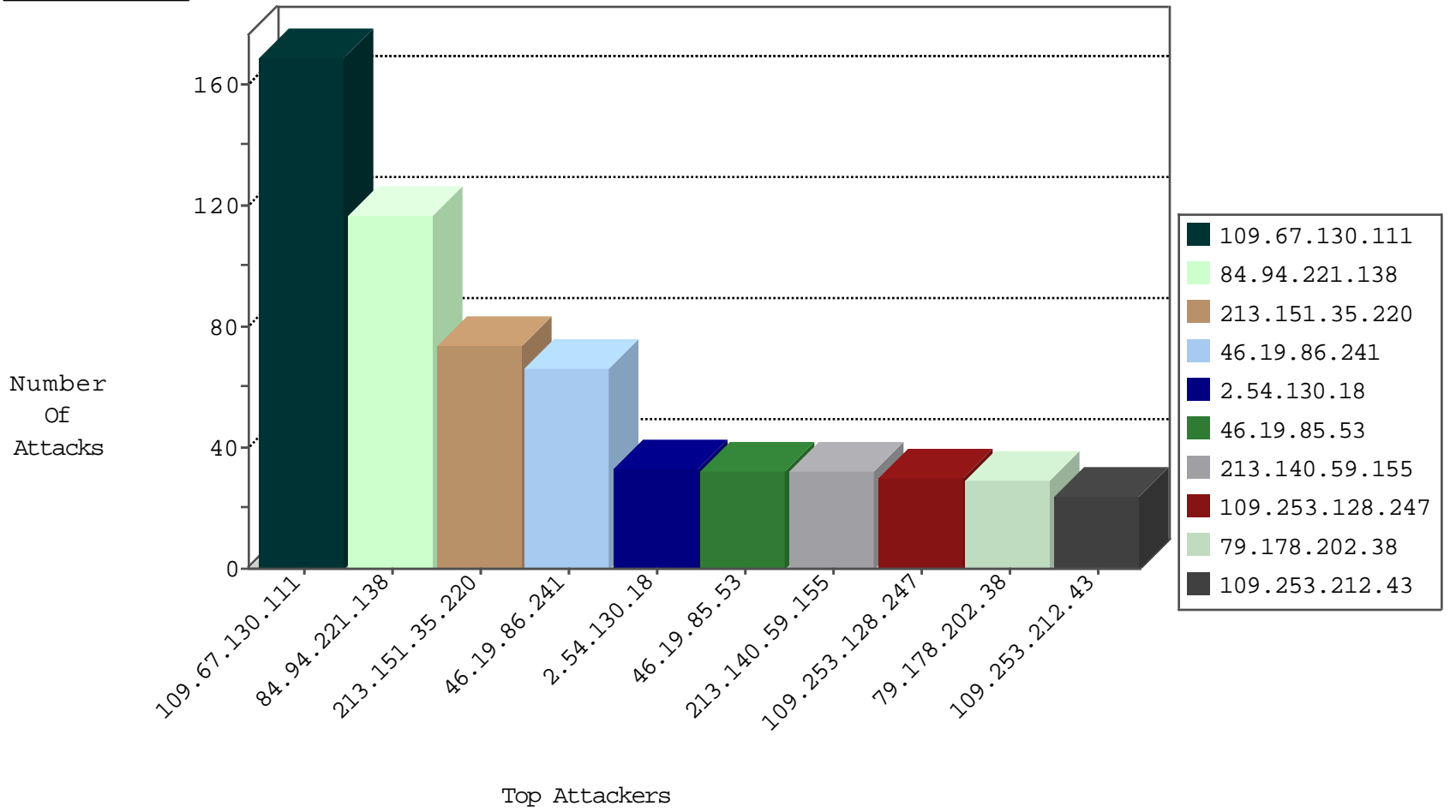
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.16.71	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
80.246.138.196	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.253.195.232	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.176.197.214	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.130	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
184.105.139.122	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.72.156	aran.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.102	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.126	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.106	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
199.58.86.209	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
193.106.54.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
87.70.246.123	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
213.140.59.155	Algeria	147.237.77.216	dover.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
42.101.152.49	China	147.237.77.176	matpash.idf.il	13764: HTTP: China Chopper Malware Communication Attempt	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.69.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.132	France	147.237.77.226	www.chamatz.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.210.194.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
37.46.38.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.80.155.214	147.237.76.86	United States	navy.idf.il	Tehila - Perl LWP with fake user agent	1
5.28.148.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.30.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.55.54.58	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
171.98.40.96	147.237.77.216	Thailand	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.190.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.189.26.18	147.237.77.216	Austria	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.30.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.40.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
13.75.95.104	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.185	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.135.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.12.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.146.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.144.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.35.51.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.17.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.140.59.155	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.94.221.138	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	117
2.54.130.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
79.178.202.38	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	20
46.19.85.53	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
79.182.230.155	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.8.193	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
176.13.13.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.164.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.178.202.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
199.203.215.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.81.35.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.164.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.127	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.84	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.159	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.6.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.183.133	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
96.47.68.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.183	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.95	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.6.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
199.203.215.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.32.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.149.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.29.76.74	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.32.22	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	5
80.246.136.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
176.106.46.74	Palestinian Territory Occupied	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
80.246.136.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.80	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
132.74.244.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.60.232.57	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.148.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.130.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	169
213.151.35.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.19.86.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
109.253.128.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.212.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.54.184.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
213.140.59.155	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-en/dover.aspx	Block	18
46.19.86.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
176.13.7.216	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	7
212.199.57.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
133.127.68.152	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.86.117	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	4
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	4
109.253.194.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.139.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.140.59.155	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.140.59.155	Block	3
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.140.59.155	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/dover.asp	Block	2
79.176.129.76	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
89.138.123.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.199.251.235	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
82.166.130.215	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.26.148.161	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
133.127.68.253	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19405-he/kkkkkkk=c3af4bd9kkkkkkk_c3af4bd9	Block	1
133.127.68.150	Japan	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
87.69.158.111	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
42.101.152.49	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
81.218.251.252	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.23	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
37.26.147.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.228.177.138	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.228.177.138	Block	1
188.116.198.78	Bahrain	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
133.127.68.150	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
42.101.152.49	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/plus/laobiao.php	Block	1
2.54.46.100	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.143	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71545.pdf	Block	1
46.19.85.95	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.148.150	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.228.177.138	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
79.182.136.29	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
188.116.198.78	Bahrain	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
133.127.68.151	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.65.77.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/general.aspx?docid=70911	Block	1
213.140.59.155	Algeria	147.237.77.216	dover.idf.il	Admin Blocking	Block	1