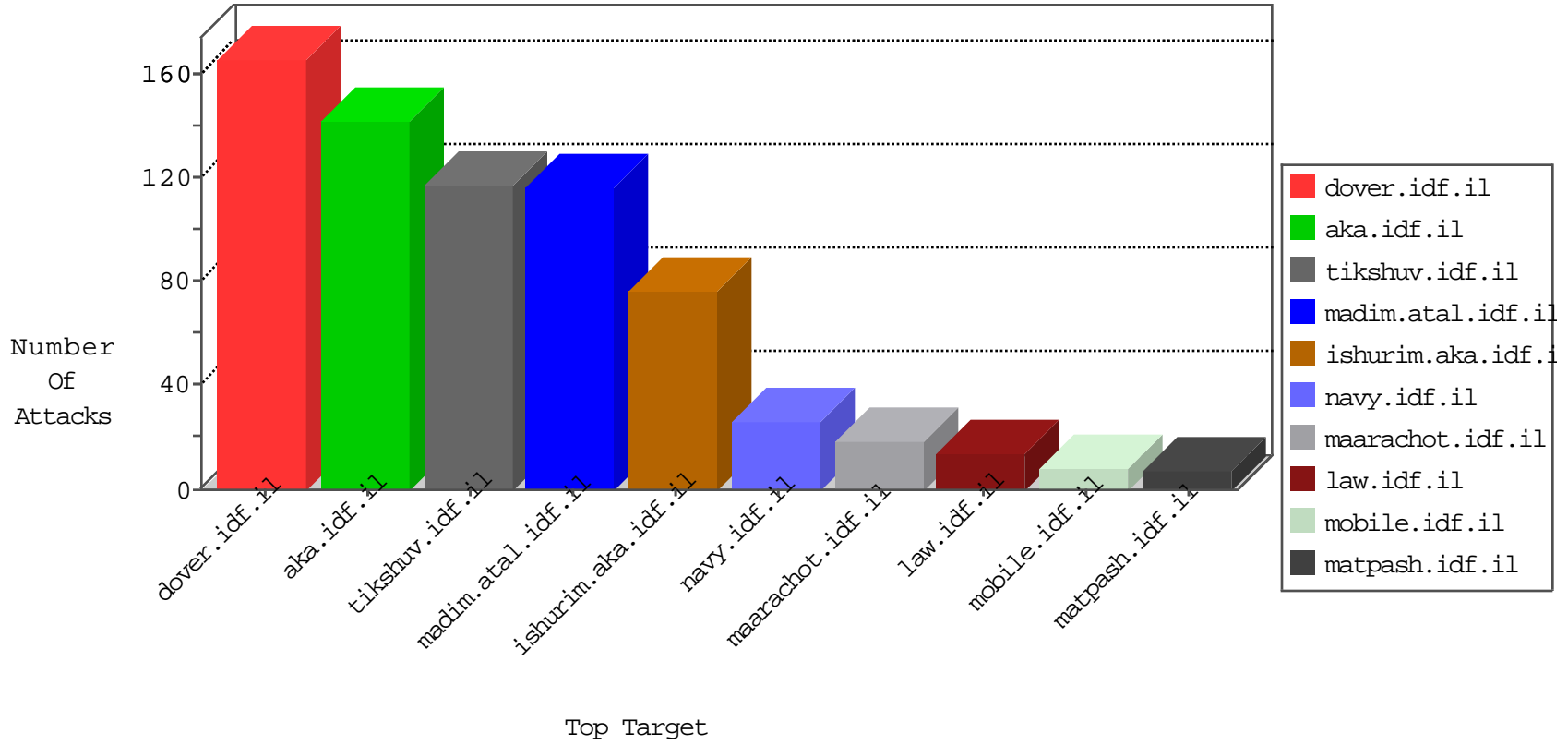


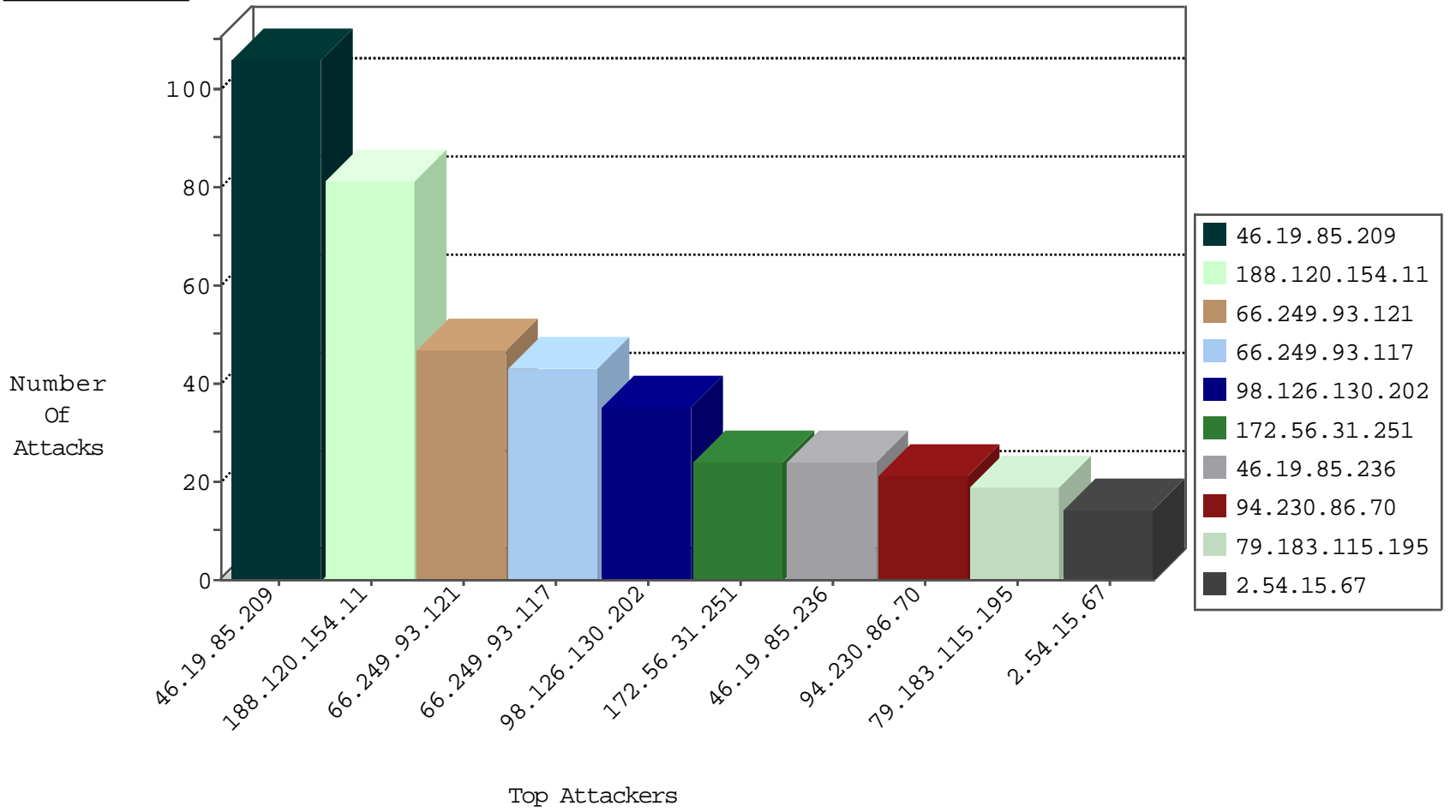
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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
141.255.164.234	Switzerland	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
141.255.164.234	Switzerland	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
116.48.235.20	Hong Kong	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
98.27.225.40	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
136.243.48.82	Germany	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Http	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
98.126.130.202	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	8
37.26.149.197	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.93.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
61.135.189.69	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
5.29.224.142	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.9.85.4	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.15.234	France	147.237.77.216	dover.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
198.20.69.74	United States	147.237.76.201	e.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
218.57.11.7	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
199.255.137.113	147.237.77.19	Belgium	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
218.57.11.7	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
198.20.69.74	147.237.76.201	United States	e.atal.idf.il	ET DROP Dshield Block Listed Source	1
179.43.141.234	147.237.77.243	Switzerland	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.120.154.11	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	40
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	31
172.56.31.251	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
190.46.50.45	Chile	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
109.65.181.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.15.67	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.236	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.236	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.6.119.234	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.154.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.142.64.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.15.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.187.113.51	Germany	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
149.88.102.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.53.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.108.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.20.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.214.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.29		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.138	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
31.154.254.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.73.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
209.140.44.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.132	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.132	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
87.70.21.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
183.206.168.57	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.73.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.3.147.108	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.132	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.70.21.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.137	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.159.209.119	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
98.126.130.202	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 98.126.130.202	Block	25
79.183.115.195	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.115.195	Block	19
94.230.86.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/general.aspx	Block	9
94.230.86.70	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 94.230.86.70	Block	3
94.230.86.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/default.aspx	Block	3
46.19.86.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.30.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.144.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
94.230.93.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/general.aspx	Block	2
94.230.93.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/general.aspx	Block	2
94.230.86.70	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/default.aspx	Block	2
94.230.93.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/general.aspx	Block	2
94.230.86.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
94.230.93.58	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.197.175.188	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
188.165.15.234	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
24.228.134.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.253.147.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
94.230.93.122	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
94.230.93.77	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/miyun/miyunselectquestionnaire.aspx	Block	1
37.142.68.55	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
185.82.200.91		147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
94.230.93.39	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.230.93.0	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
109.64.102.148	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
94.59.135.79	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
94.230.93.61	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	1
66.249.64.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/gyus/forum/asp/showforum.asp	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzyy	Block	1
141.212.122.209	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
94.230.93.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/	Block	1
31.154.254.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
97.32.140.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
66.249.66.137	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/924-2744-he/patzar.aspx	Block	1
94.230.93.80	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/priotfindanswer.aspx	Block	1
40.77.167.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.24.109.28	Romania	147.237.77.74	law.idf.il	PHP Attempt	Block	1
94.230.93.48	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.230.93.0	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.65.181.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
94.230.93.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/default.aspx	Block	1
94.230.93.61	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
198.58.102.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
37.26.146.246	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
183.206.160.57	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 183.206.160.57	Block	1
94.230.93.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
98.126.130.202	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 98.126.130.202	Block	1