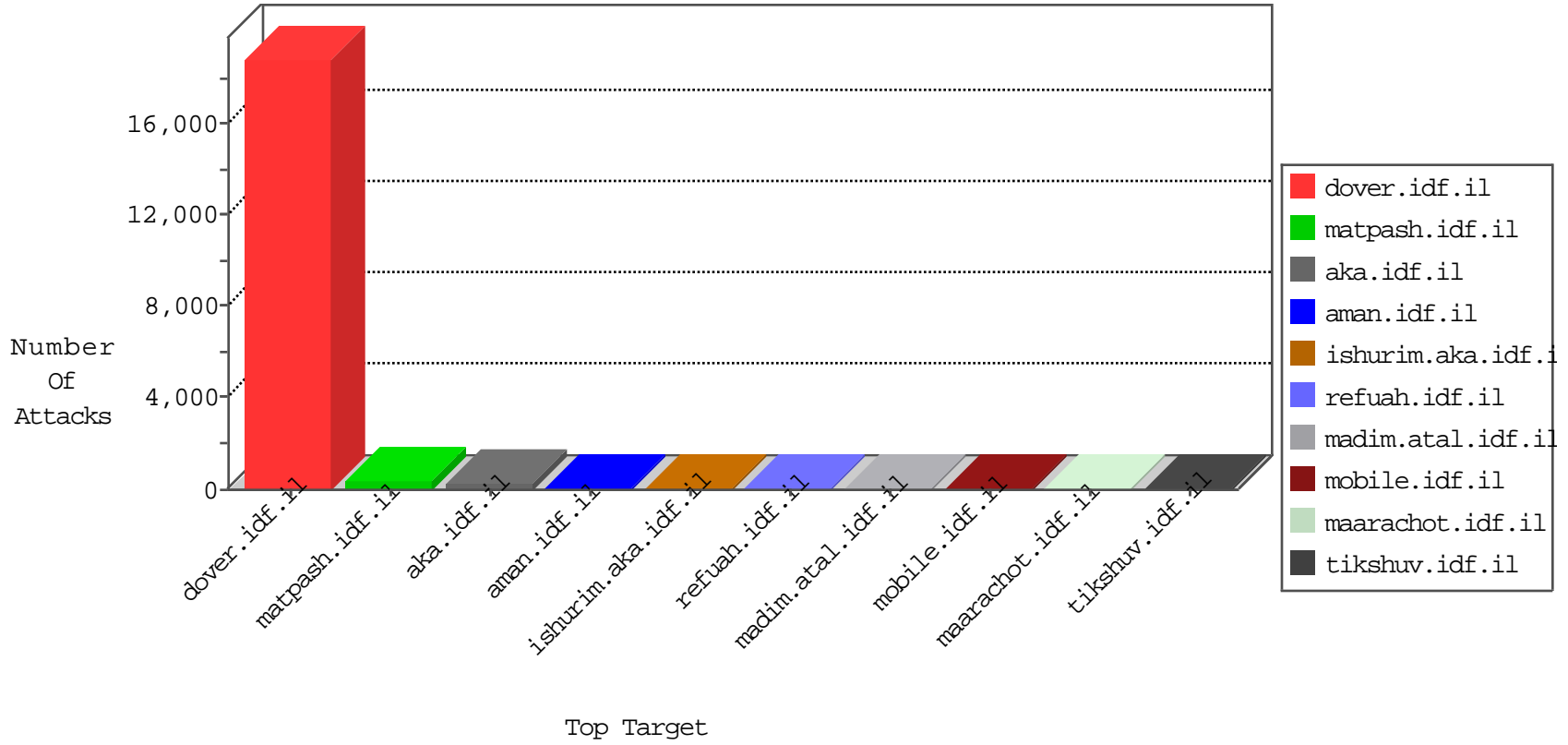
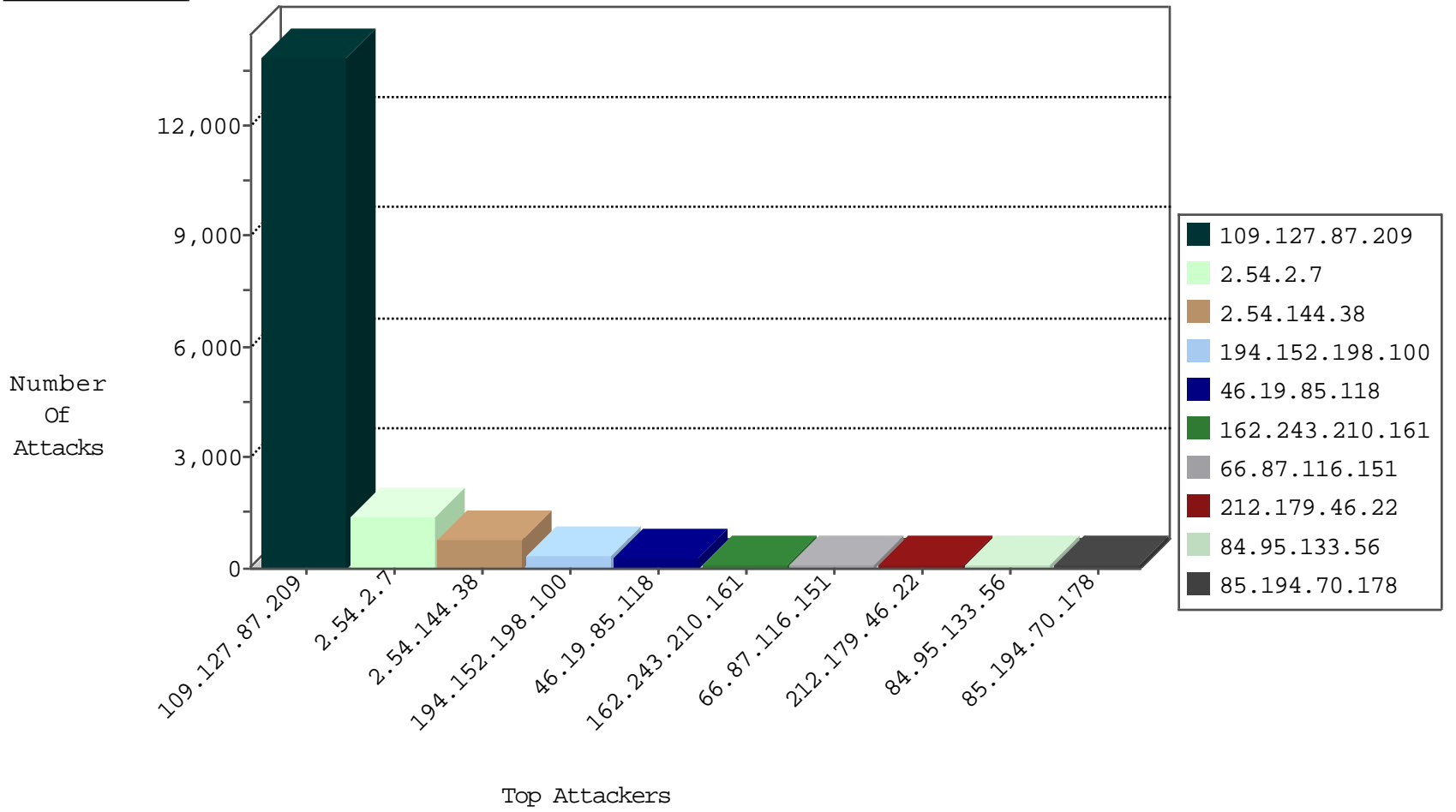


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
109.127.87.209	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4482
213.8.71.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	261
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	79
109.64.145.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
2.52.128.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
109.253.156.64	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
109.127.87.209	Iraq	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	8
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
93.172.143.152	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
199.30.24.57	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
79.183.207.156	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
176.12.147.135	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.177.184.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
46.120.5.103	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.177.144.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
2.54.7.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.183.207.156	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
85.250.6.244	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.52.174.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.32.179.61	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
31.168.151.101	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.19.33	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
212.199.251.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
41.176.120.133	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
85.250.6.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.183.111.240	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.175.97	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.52.174.238	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
10.0.0.4		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.142.100.150	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
46.120.229.69	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
149.78.5.229	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
109.253.137.15	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
82.80.180.46	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.103	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.177.159.41	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.59	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.116.211.238	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.49.226	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.146.236	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.16.3	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
109.64.117.150	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
95.173.171.236	Turkey	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
84.228.243.86	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	ET WEB_SERVER Poison Null Byte	1
222.186.56.103	China	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.59	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.175.170	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
119.90.139.71	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
109.253.132.67	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.174.92	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
103.244.204.18	Indonesia	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
84.229.148.229	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.127.87.209	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13790
2.54.2.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1394
2.54.144.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	753
194.152.198.100	Croatia	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	338
46.19.85.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	266
162.243.210.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	90
66.87.116.151	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	89
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	87
84.95.133.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
85.194.70.178	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
77.125.214.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
91.231.92.29	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
192.115.90.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
107.77.70.25	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
84.111.184.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
79.183.207.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
84.109.111.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
176.58.108.28	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
109.127.87.209	Iraq	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	28
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
213.151.54.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
67.194.229.137	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
176.12.149.254	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
178.63.165.187	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
207.241.237.106	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
80.246.133.79	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	18
37.26.147.240	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
87.68.154.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
84.108.3.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
212.179.49.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
2.54.6.144	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
189.143.244.249	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
181.250.21.4	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
84.228.59.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
180.217.30.181	Taiwan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
188.120.148.132	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	13
2.54.7.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.64.35.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
31.186.228.170	United Kingdom	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
2.54.170.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.86.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
2.54.60.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.142.68.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.68.209	Block	39
37.26.147.240	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	8
79.182.183.148	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	6
68.172.239.146	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
93.172.144.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	4
37.142.221.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
79.182.29.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
46.117.0.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
87.68.240.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	3
213.151.61.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.12.139.229	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.179.139.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.65.122.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.120.110.253	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
109.253.139.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
62.219.128.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.39.170	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
5.28.136.43	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/homefront/hebrew/default.stm	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14662-he/dover.aspx	Block	1
176.12.139.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
109.64.146.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
84.228.93.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.68.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
2.52.62.234	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.12.151.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.78.198	Israel	147.237.76.31	nakhal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
141.212.122.26	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
66.249.64.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
41.250.66.43	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/	Block	1
5.29.91.170	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19072-he/dover.aspx	Block	1
85.65.103.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
2.54.6.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.119	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
141.212.122.26	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
79.183.134.17	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
31.186.228.170	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0104.stm	Block	1
176.12.140.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.138.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
46.121.69.197	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.190.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.100.150	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cp in www.aka.idf.il/main/gyus/userdetails/updateuserdetails.aspx	None	1
2.54.134.49	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
193.43.244.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.61.53	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1