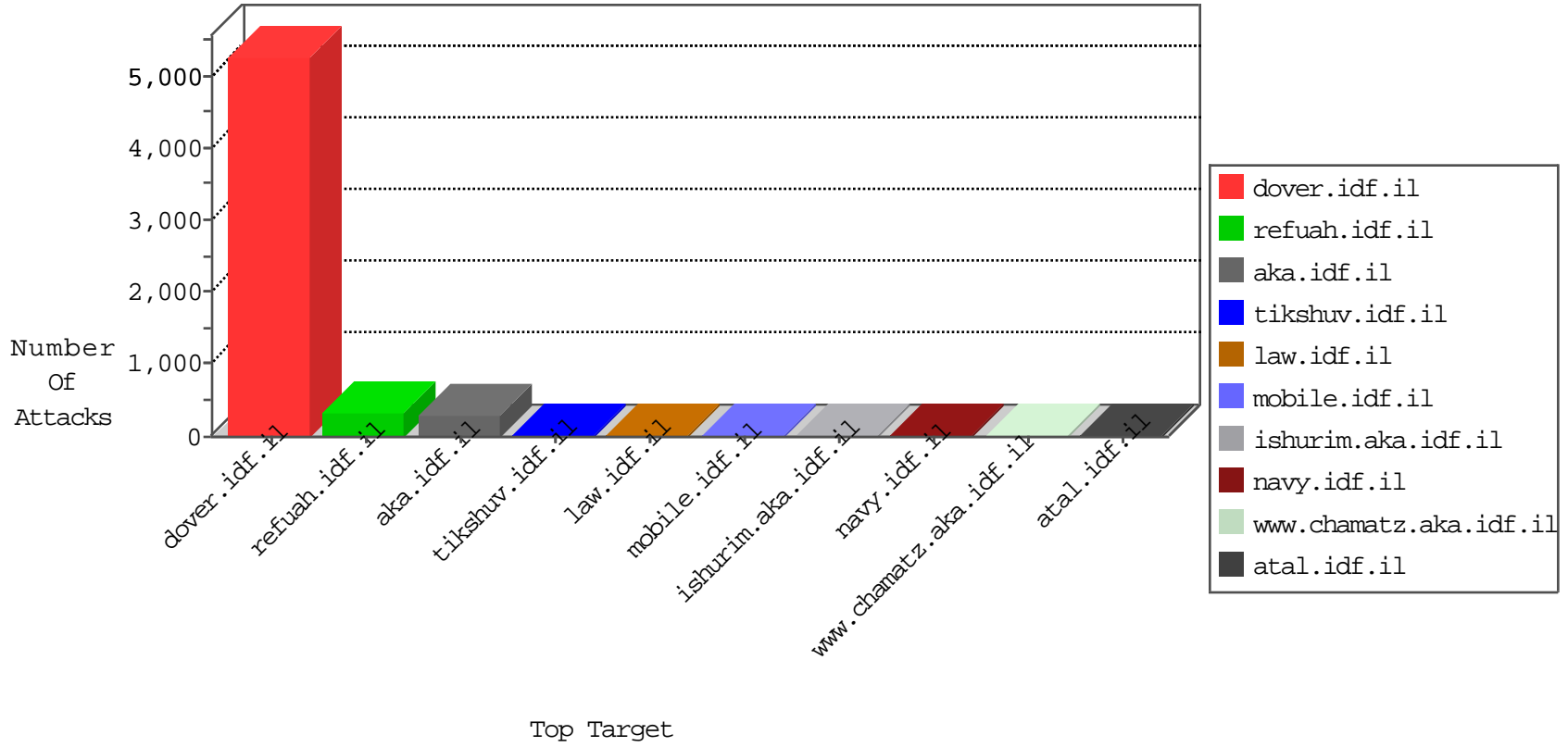
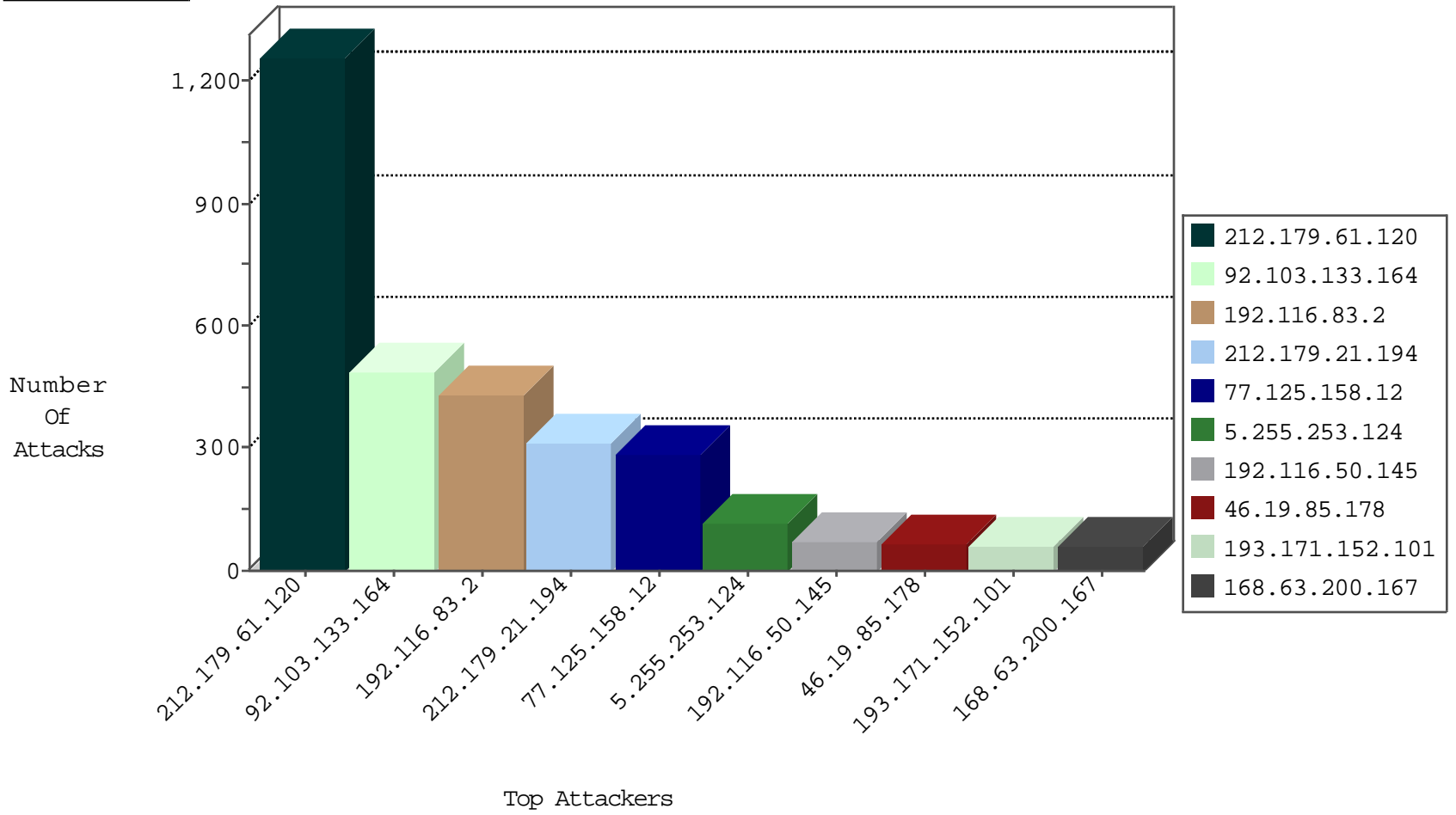




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	252
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
192.3.207.66	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
84.108.204.60	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.3.207.66	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.121.211.116	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
41.185.12.165	South Africa	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
176.228.139.239	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	2
79.181.30.117	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.178	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.38	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.59	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
46.121.244.2	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
178.15.92.114	Germany	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.96	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.169	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
213.8.58.181	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
212.179.61.120	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.126.158	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.139.239	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
121.88.5.177	Korea, Republic of	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
116.90.232.142	Nepal	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.178	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.67	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.50.2.105	Korea, Republic of	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
37.26.146.161	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.117.136.8	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
5.29.48.197	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
193.107.16.206	Russian Federation	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
176.12.136.4	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
119.90.139.72	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
104.197.27.68		147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
80.178.116.1	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
62.0.105.133	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
222.69.94.13	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.208	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
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1249
92.103.133.164	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	484
192.116.83.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	433
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	310
77.125.158.12	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	286
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	110
192.116.50.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
46.19.85.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
193.171.152.101	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
168.63.200.167	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
213.8.96.180	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	57
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
212.116.163.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
2.52.29.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
213.8.159.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
80.178.114.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
82.166.146.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
31.168.133.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
212.143.56.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
85.250.146.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
212.179.212.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
70.199.68.84	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
213.151.32.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
37.26.148.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
193.34.57.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
37.26.147.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
132.70.66.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
84.108.26.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
84.228.100.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
37.26.148.251	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
81.218.151.163	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
62.0.224.1	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	17
80.179.223.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
87.69.97.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
93.172.171.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
212.179.241.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
212.143.3.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
220.237.125.113	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
95.86.99.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
213.151.53.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
94.153.9.66	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	4
213.151.48.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.64.112.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	3
46.121.68.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.21.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
77.125.79.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.130.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
132.70.66.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
62.219.86.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.86.253	Block	2
46.19.85.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
192.114.86.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.101.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
46.121.211.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
141.212.121.152	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
2.54.135.243	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
213.57.50.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.180.8.153	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
176.12.137.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.7	Block	1
62.219.86.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
46.19.86.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.160.156.56	Israel	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.80.19.145	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/doctrine/ethics.stm	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
46.121.244.2	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
141.212.121.152	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
2.54.168.135	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.228.139.239	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
79.180.138.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/x@x\$*xax™xª 9	Block	1
46.19.86.195	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
109.253.147.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
199.30.25.191	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1