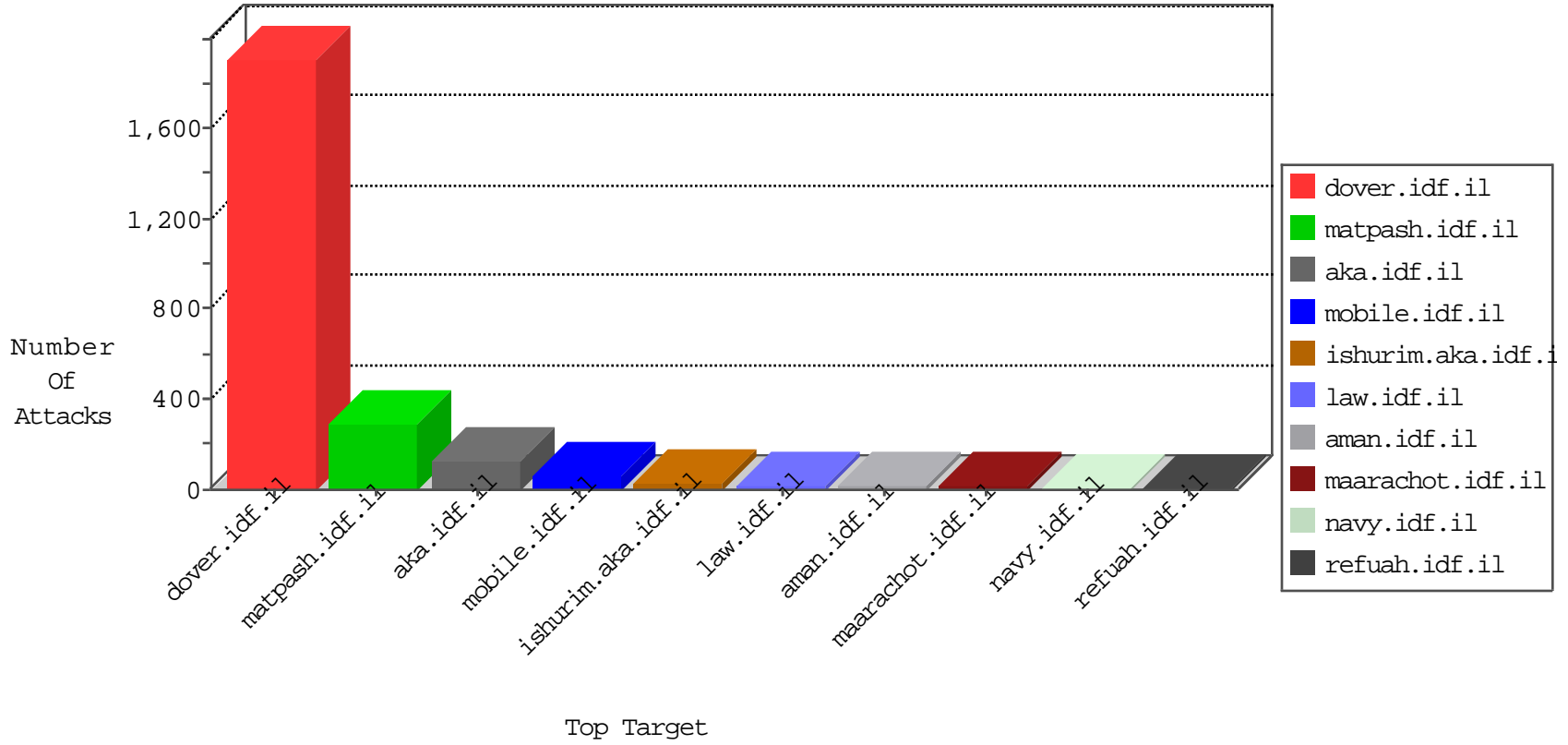
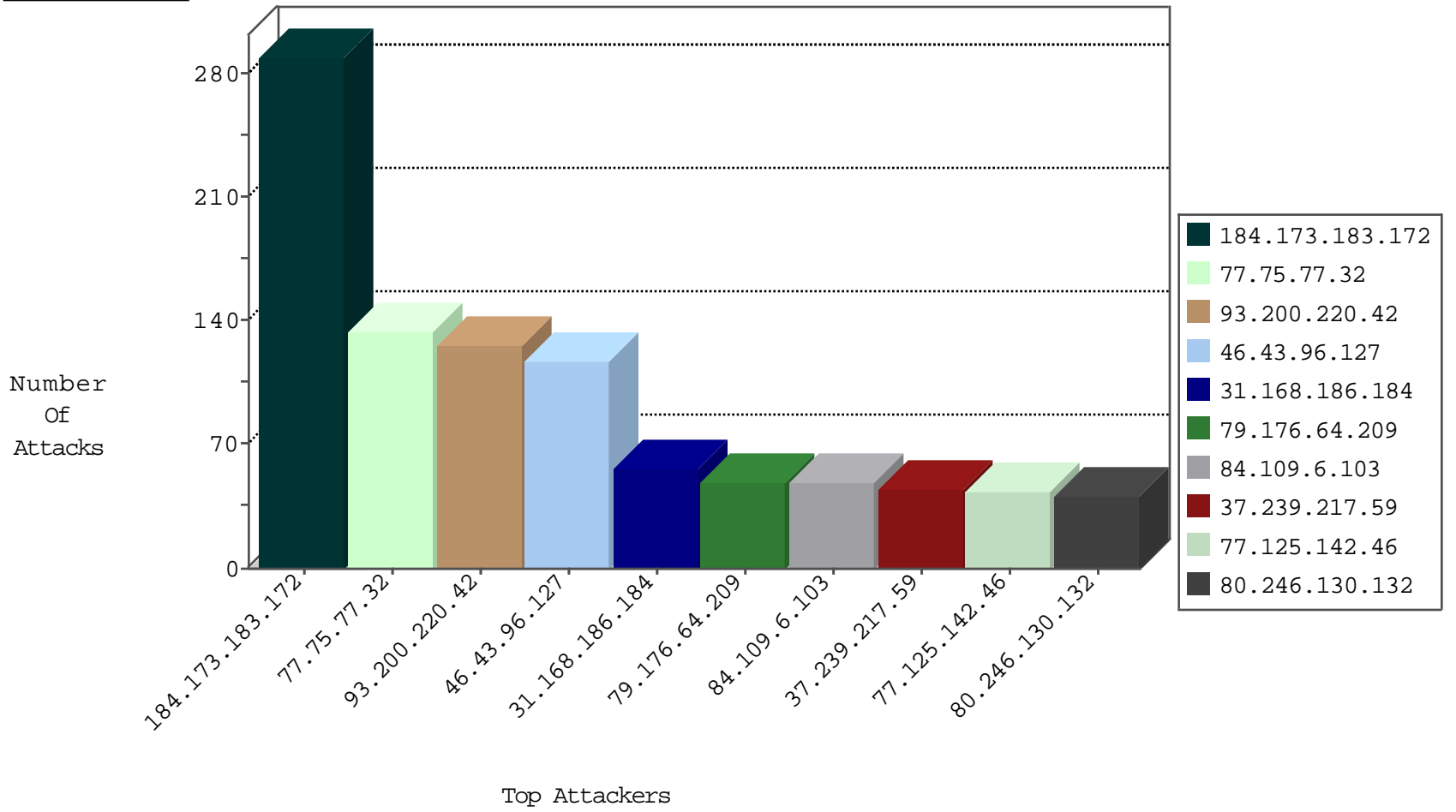


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7285
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	852
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	822
220.181.108.75	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	251
84.109.14.123	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	159
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	154
85.64.103.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
87.69.86.98	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
79.178.151.216	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	5
79.178.151.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.121.90.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
10.10.1.11		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
37.142.253.27	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
134.147.203.115	Germany	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2
10.10.1.11		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
84.94.200.111	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
46.19.85.137	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
46.19.85.137	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
190.23.168.246	Paraguay	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	290
37.46.39.80	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.177.99.251	Israel	147.237.72.166	aka.idf.il	EgovRep_B-N_70-99	Block	2
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.76.198	e.yohanan.idf.il	DVRep_B-N_60_100	Block	1
5.29.19.130	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	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
5.29.202.12	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
37.26.147.143	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.64.176.215	Israel	147.237.72.156	aman.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
99.59.186.184	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	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	6
66.249.64.57	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.163	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
183.232.128.156	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
87.69.0.167	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
178.32.251.100	France	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
87.69.85.15	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.163	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.243.221.215	Portugal	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
77.75.77.32	Czech Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	134
93.200.220.42	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	127
46.43.96.127	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	117
31.168.186.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
79.176.64.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
37.239.217.59	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
77.125.142.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
99.238.32.134	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
80.246.130.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
106.139.7.173	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
188.27.71.121	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
84.228.50.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
149.78.22.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
84.228.140.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
79.179.60.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
46.19.86.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
84.109.6.103	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
75.126.221.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
176.12.146.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
37.26.147.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
37.218.218.30	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
5.29.101.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
217.66.234.144	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
85.64.58.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
79.180.231.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.12.138.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.253.128.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
200.93.232.43	Ecuador	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.64.60.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
180.191.224.245	Philippines	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.255.225.97	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
5.28.149.115	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	10
46.116.202.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
98.210.231.138	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
208.69.40.107	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
84.109.202.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.26.148.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.19.85.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
79.183.137.87	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	4
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.66.153.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
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
149.78.210.85	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	2
109.66.153.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	2
84.228.157.215	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	2
85.64.157.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.183.55.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.93.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	2
84.94.36.159	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.156.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
93.173.240.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.160.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gen204	Block	1
190.23.168.246	Paraguay	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 190.23.168.246	Block	1
157.55.39.163	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/333-he/patzar.aspx	Block	1
157.55.39.24	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/331-he/patzar.aspx	Block	1
109.66.24.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
66.249.69.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.28.149.115	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
157.55.39.222	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/336-he/patzar.aspx	Block	1
84.109.232.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.9.148	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.253.156.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.59.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
54.209.60.63	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/forms	Block	1
190.23.168.246	Paraguay	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/spanish/	Block	1
80.246.133.115	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.164	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/453-he/patzar.aspx	Block	1
77.125.123.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.5	Block	1
5.29.18.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.150.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.111.15.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.186.231	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal/natziv.stm	Block	1
109.64.59.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-7909-he/idfgdover.aspx	Block	1
193.16.101.145	Ukraine	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
157.55.39.190	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/204-he/patzar.aspx	Block	1
80.246.137.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
77.125.135.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1408-he/atal.aspx	Block	1
31.168.193.8	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1