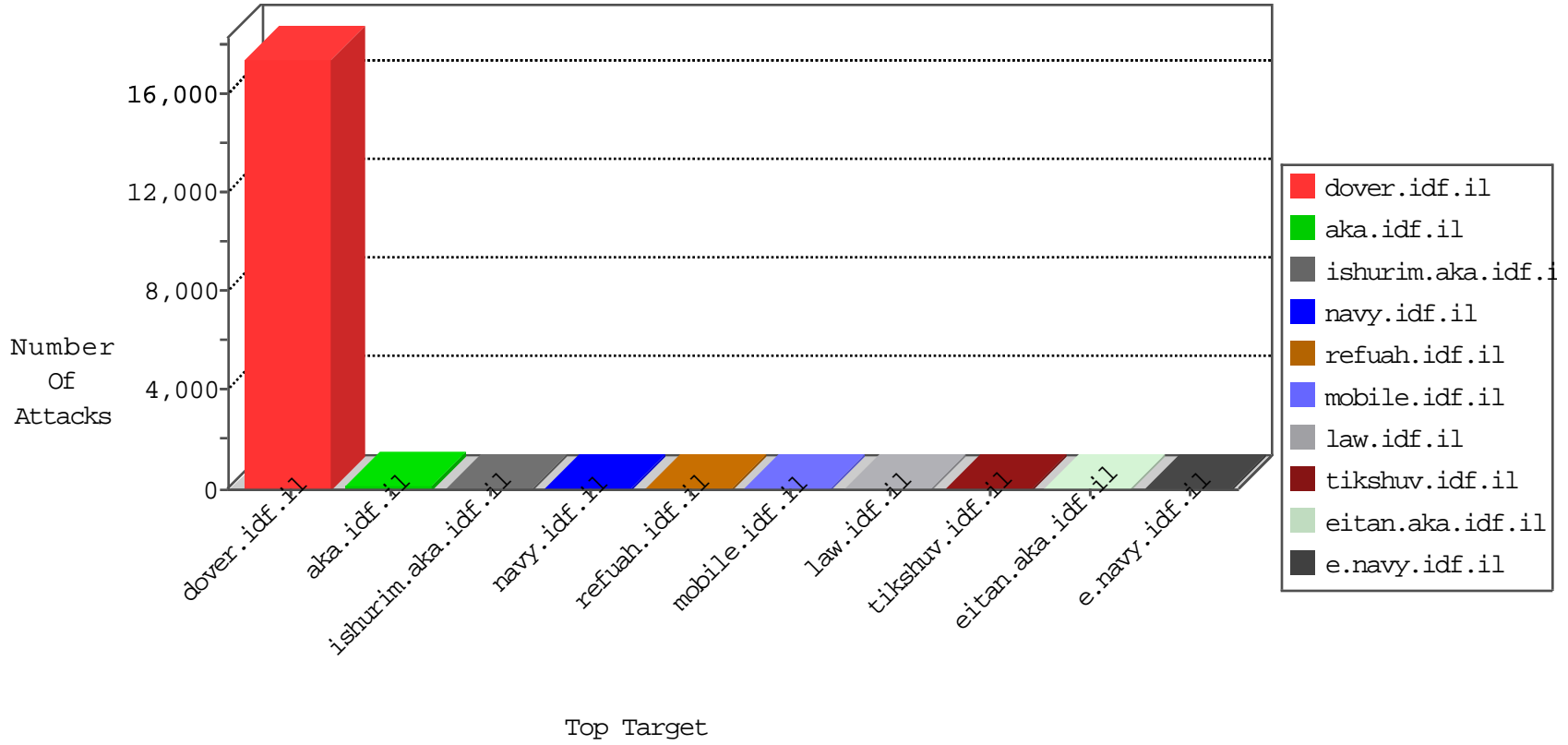
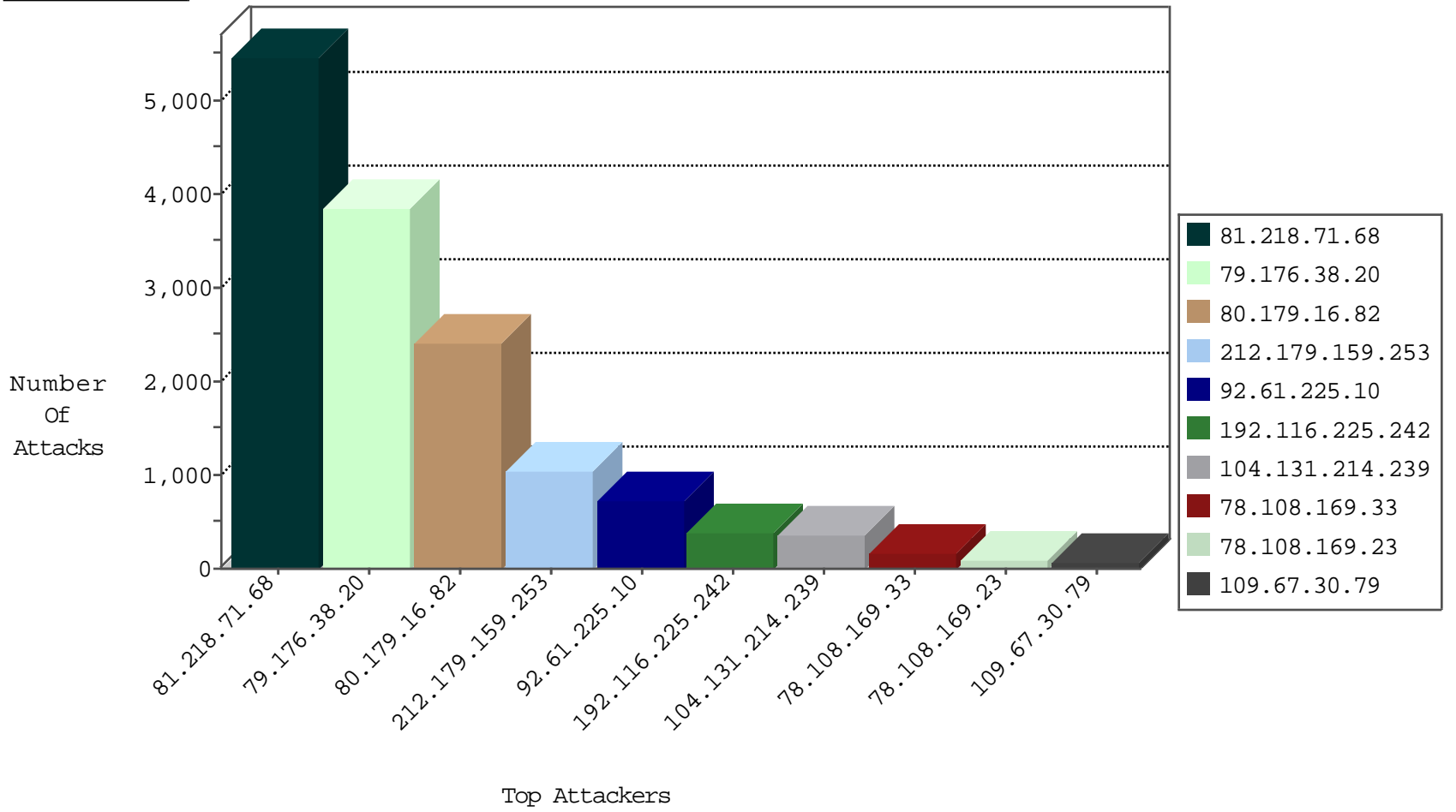




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
81.218.71.68	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2811
212.143.44.5	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
2.54.146.133	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
46.19.85.88	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
46.19.86.93	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
46.117.221.38	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
212.179.221.25	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
192.168.10.49		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.179.33.107	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
10.20.118.134		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
60.34.124.42	Japan	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
2.54.23.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.116.225.242	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
109.72.152.167	Ukraine	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
10.20.118.134		147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
2.52.13.7	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.80.219.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
211.14.225.111	Japan	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
104.131.214.239		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	19
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	2
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	2
93.120.27.62	Romania	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.17	m.ny-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
2.52.23.32	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.233	atal.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
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
213.57.167.63	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
184.168.139.128	United States	147.237.8.50	e.tikshuv.idf.il	EgovRep_B-N_70-99	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
84.108.165.48	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	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
184.168.139.128	United States	147.237.76.39	mobile.meitav.idf.il	EgovRep_B-N_70-99	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.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
198.20.69.98	United States	147.237.76.176	test.ncore.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	1
80.246.133.199	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
78.129.148.77	United Kingdom	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
1.241.229.116	Korea, Republic of	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
212.179.155.129	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.134.5	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.16.82	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
1.241.229.116	Korea, Republic of	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
212.179.221.25	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
81.218.71.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5459
79.176.38.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3851
80.179.16.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2415
212.179.159.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1038
92.61.225.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	732
192.116.225.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	377
104.131.214.239		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	355
78.108.169.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	146
78.108.169.23	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	84
109.67.30.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
79.179.123.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
212.179.221.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
109.253.88.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
192.117.170.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
62.210.167.112	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
46.116.194.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
37.26.146.178	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
68.4.56.253	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
46.19.86.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
109.253.159.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.19.85.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
109.186.185.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
2.52.162.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
85.64.216.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.116.189.197	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	20
132.68.113.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
78.108.161.226	Lebanon	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	20
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.73.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	19
212.143.76.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
31.186.228.27	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
91.231.192.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.73.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
80.246.130.198	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	15
31.186.228.62	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.134.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
212.199.121.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
2.52.129.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
82.145.218.194	Europe	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.96	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.129.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.179.21.194	Israel	147.237.77.74	law.idf.il	Suspicious Response Code	Block	2
164.138.122.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	2
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 212.117.143.250 (Unknown SSL Session)	None	2
109.253.134.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1317-he/refuah.aspx	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	1
66.249.64.187	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
184.105.247.196	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
81.218.251.250	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.73.205	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1879	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.67.79	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.141	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/894-7860-he	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-index10.stm	Block	1
66.249.73.197	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.73.197	Block	1
66.249.64.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
185.32.178.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.158.139.101	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.166.209	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.73.213	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.73.213	Block	1
216.218.206.67	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/913-692-he/patzar.aspx	Block	1
46.19.85.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.34.228	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmi	Block	1
31.44.140.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
217.69.133.244	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/c	Block	1
66.249.67.105	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6447-he/patzar.aspx	Block	1
66.249.64.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
184.105.247.195	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
80.246.130.198	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
212.117.143.250	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.64.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
132.64.53.158	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
31.168.71.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
66.249.67.139	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
66.249.64.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
184.105.247.196	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
81.218.56.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/shonot/meida/noinformation.stm	Block	1
212.143.90.173	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20535-he/dover.aspx	Block	1
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
31.168.185.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1