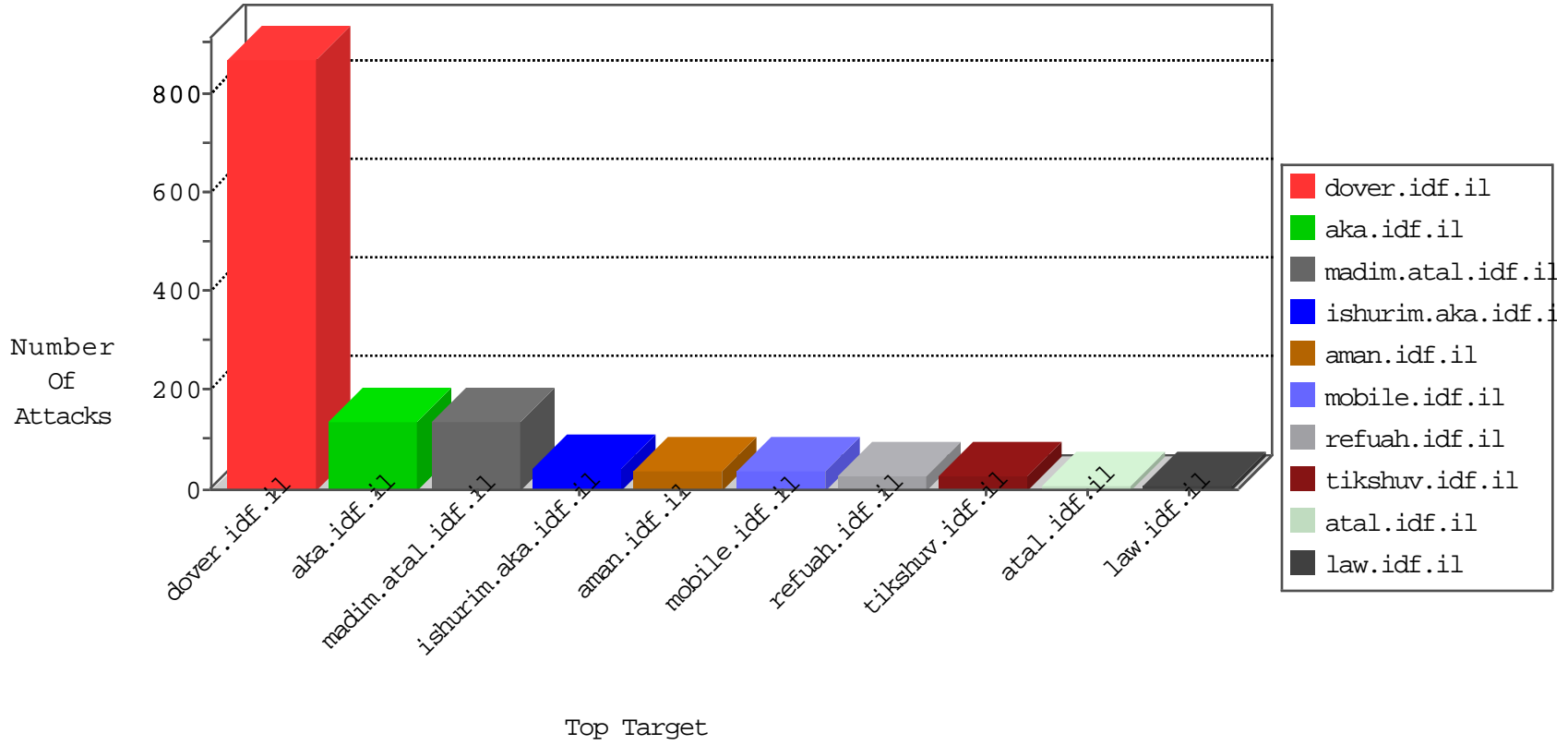
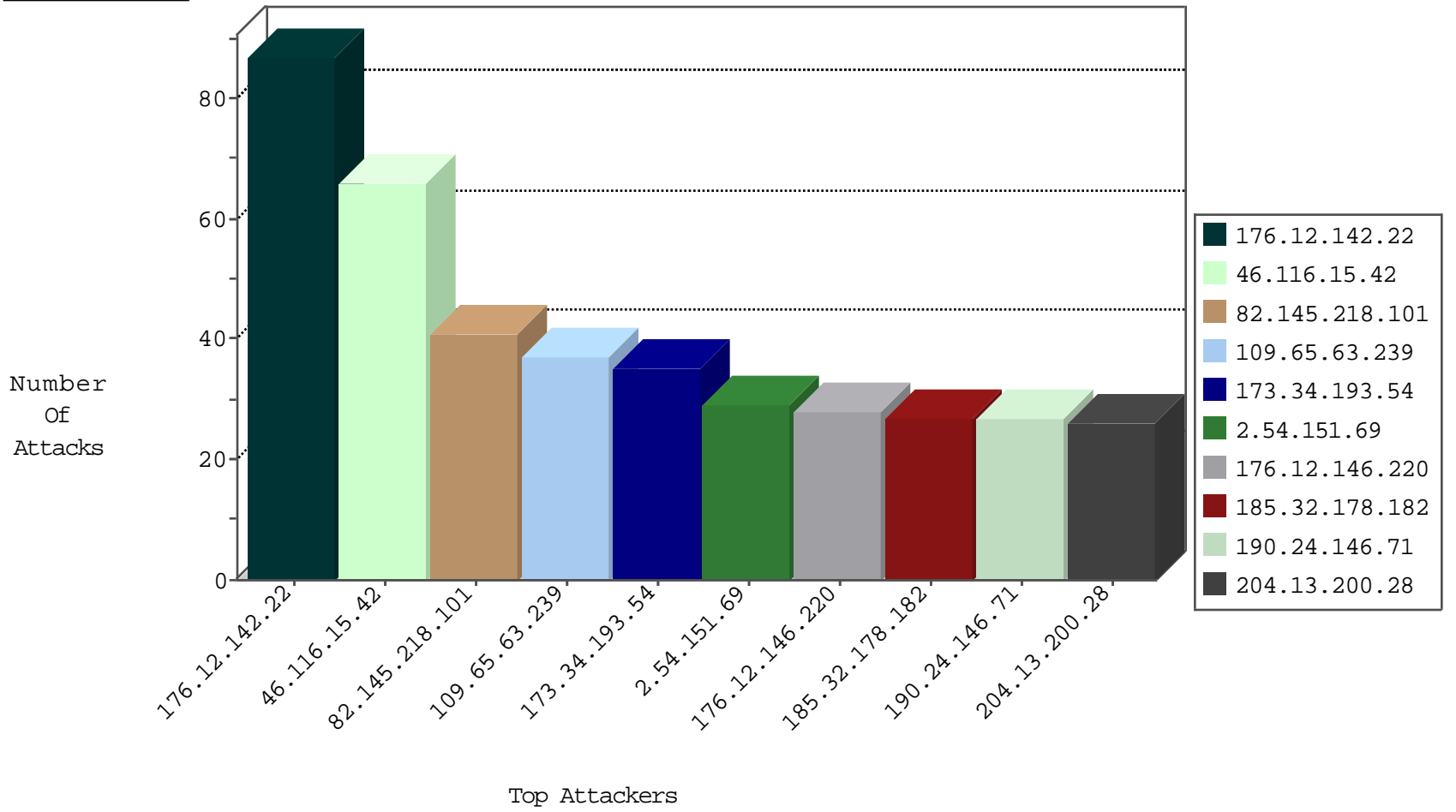




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	346
176.12.146.220	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
79.181.52.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
109.64.188.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
10.0.0.2		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.65.105.192	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	4
84.109.185.165	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.145.218.101	Europe	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
50.204.241.108	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
2.54.185.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.108.70.52	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.184	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
111.202.66.66	China	147.237.0.17	m.ny-kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	1
84.110.209.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.184	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
111.202.66.66	China	147.237.8.45	e.eitan.idf.il	L4 Source or Dest Port Zero	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
197.37.115.59	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.109.197.38	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.197	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.207	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.212	e.dover.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
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.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
79.181.102.113	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.37.180	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.236	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.205.123	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
121.46.0.125	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.205.123	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
221.133.0.27	Vietnam	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
221.133.0.27	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.154	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	1
218.89.137.3	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.19.107.114	Poland	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.205.123	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
121.46.0.125	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.133.0.27	Vietnam	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.133.0.27	Vietnam	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
221.133.0.27	Vietnam	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.152	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.89.137.3	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.149.240.162	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.88.5.177	Korea, Republic of	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.116.15.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
82.145.218.101	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
109.65.63.239	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
173.34.193.54	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
185.32.178.182	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
50.75.251.214	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
46.19.85.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
82.81.240.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.19.85.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
84.111.192.168	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
79.177.201.18	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
37.142.11.125	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
185.13.195.150	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	13
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
197.96.72.154	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.228.3.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
192.117.173.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
89.138.12.33	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.179.141.191	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
176.12.149.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.176.155.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.179.141.191	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
79.178.36.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
94.230.86.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
81.218.172.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.66	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
31.186.228.60	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.66.34.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
94.230.86.175	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
79.183.231.100	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
82.102.141.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.108.14.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
80.246.130.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
31.186.228.86	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.179.141.191	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
85.64.156.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.178.58.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.183.231.100	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
216.223.27.61	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.142.22	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.142.22	Block	86
2.54.151.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
109.253.135.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
87.69.200.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
95.131.110.106	United Kingdom	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
77.126.215.190	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.57.215.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
72.225.197.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.76.101.127	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	2
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.83.148	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.69.146.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.27.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
37.142.11.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.190.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.141.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
176.67.126.126	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-en	Block	1
79.181.186.226	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan	Block	1
149.78.234.184	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.139.162.7	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
84.111.192.168	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
5.255.253.99	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
192.116.50.115	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/69054.qdf	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx	Block	1
61.135.190.69	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
85.250.74.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
80.246.138.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.67.126.126	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
68.180.229.27	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1235-he/atal.aspx	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.228.56.217	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
24.150.155.53	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
194.187.168.19	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nahal	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-15489-he/dover.aspx	Block	1
109.253.136.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34//	Block	1
180.76.5.170	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info07.asp	Block	1
72.71.178.106	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.131.210.80		147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/default.aspx	Block	1
199.87.253.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/jenin/site/english/main_index.stm	Block	1
84.228.234.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.142.22	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
66.249.67.23	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//	Block	1