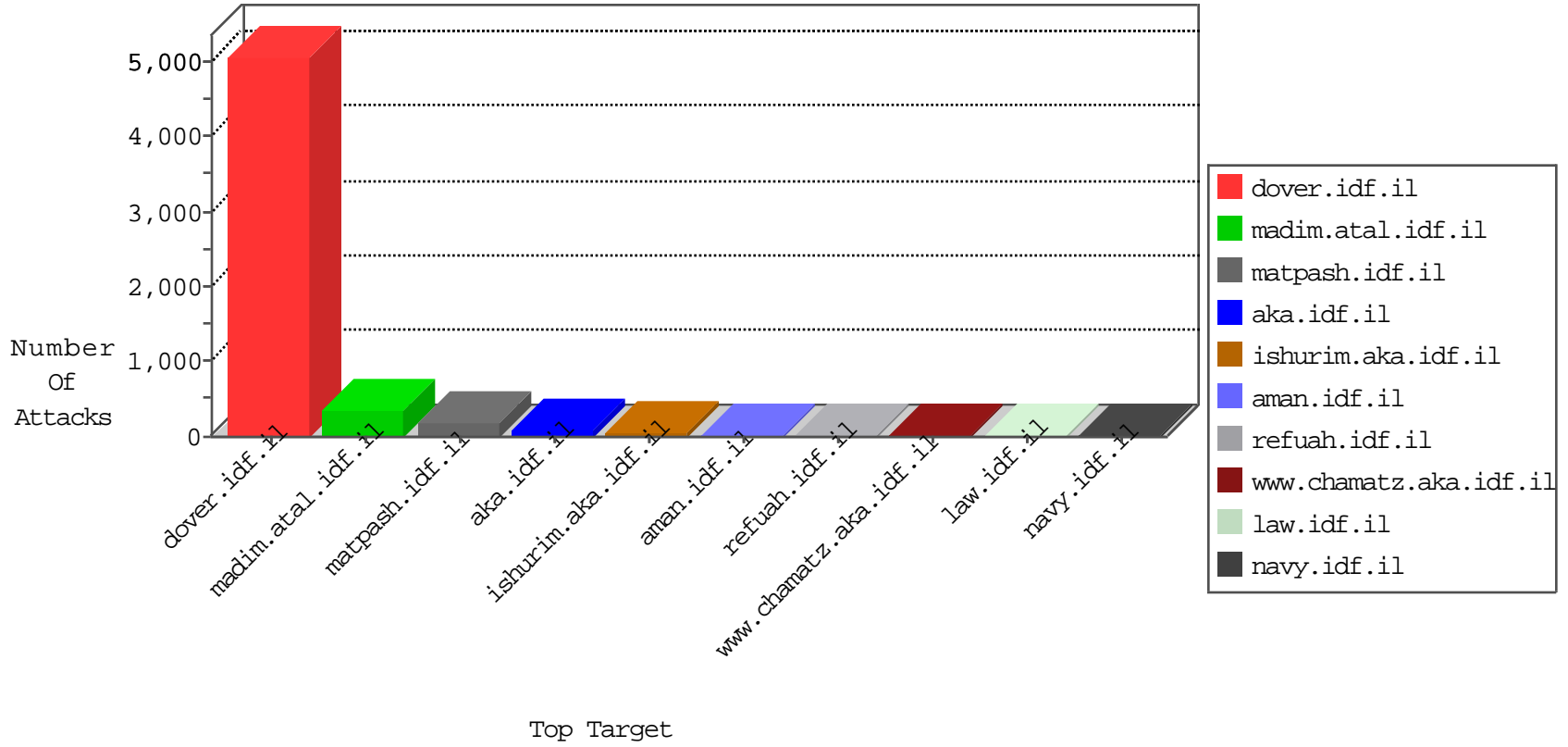
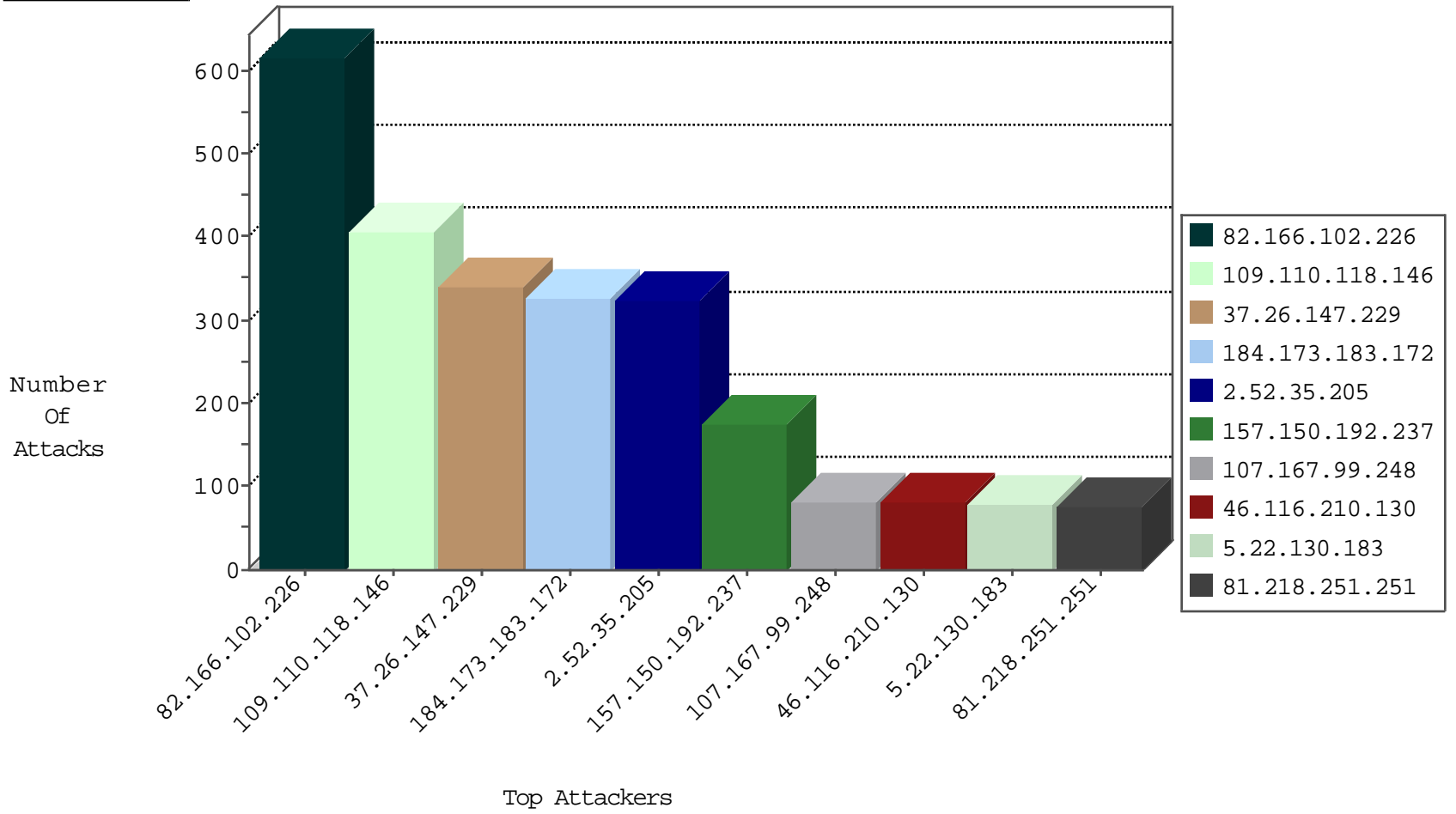


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	798
212.199.156.81	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	332
85.250.228.53	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
85.250.119.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
84.111.63.141	Israel	147.237.76.86	navy.idf.il	block-sp-trafl	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	184
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	141
185.33.168.150	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	EgovRep_B-N_70-99	Block	4
46.19.85.132	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.255	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	2
46.116.162.4	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.116.210.130	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	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
199.203.84.120	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
84.228.252.150	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
212.150.245.250	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
66.240.236.119	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.205	prisha.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
2.54.22.202	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.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
66.249.64.156	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
84.109.3.77	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.239.118.143	Chile	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -f -sS	1
61.160.224.129	China	147.237.77.216	dover.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
183.136.216.3	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
109.2.167.100	France	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.239.118.143	Chile	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.136.216.3	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
128.199.254.26	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
107.167.99.248	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.6.90	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.166.102.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	616
109.110.118.146	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	406
2.52.35.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	323
157.150.192.237	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	173
107.167.99.248	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	80
5.22.130.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	79
46.116.210.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	78
81.218.251.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	77
37.26.148.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	74
171.96.248.8	Thailand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
2.52.171.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
2.54.178.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
89.138.226.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
84.111.64.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
85.65.84.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
93.173.12.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
79.178.139.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
92.243.181.74	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
2.52.164.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
195.95.183.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
62.219.245.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
87.69.165.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
82.145.219.27	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
2.54.22.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.147.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
122.173.12.243	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
37.26.146.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
46.19.86.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
2.52.15.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
5.29.205.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
77.125.138.99	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.117.76.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
166.137.252.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
46.19.86.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
93.172.5.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
195.62.18.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.19.85.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
69.54.25.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.19.86.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
132.64.182.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
46.19.85.34	Israel	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
37.26.147.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	333
5.255.253.93	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mod	Block	4
79.180.193.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	4
213.151.50.156	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	3
2.54.42.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	3
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
157.55.39.67	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.67	Block	2
91.200.224.91	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.200.224.91	Block	2
37.26.147.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.116.162.4	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	2
2.54.30.208	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
109.186.173.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.240	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6363-he/patzar.aspx	Block	1
87.69.95.131	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/&q=xžx@x~x"x x x' x?x™xª, x-x™xª x"xžx@x~x"x" x"x x'x'x?x™xª,	Block	1
193.38.100.250	United Kingdom	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
77.125.147.191	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.73.221	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
46.120.15.215	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
105.157.167.128	Morocco	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
79.182.171.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
66.249.64.245	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
89.68.52.46	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
23.27.44.206	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
217.146.69.7	Estonia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
79.176.104.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/lomdim/forum/asp/showforum.asp	None	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
66.249.64.153	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	1
105.157.167.128	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.157.167.128	Block	1
79.183.101.190	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
2.54.132.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
209.73.137.21	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/rabanut/general.aspx	None	1
66.249.65.97	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
195.154.181.152	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/manager/	Block	1
79.177.12.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.81	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/	Block	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mazi.idf.il	Block	1
105.157.167.128	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/php	Block	1
80.246.130.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
5.102.197.38	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 5.102.197.38 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1